# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-328846
(43)Date of publication of application : 15.11.2002

(51)Int.Cl. G06F 12/14
G06F 17/60
H04L 9/08
H04L 9/32

(21)Application number : 2002-041890
(22)Date of filing : 19.02.2002

(71)Applicant : SONY COMPUTER ENTERTAINMENT INC
(72)Inventor : SHIMADA SHUGI
OKAMOTO SHINICHI
YOSHIMORI MASAHARU
INUI TSUTOMU
SHIMAKAWA KEIZO
OKADA TOYOJI
KUBO AKIRA
NAKAMURA MITSUHIRO

(30)Priority
Priority number : 2001044358 Priority date : 20.02.2001 Priority country : JP

(54) COPY MANAGEMENT SYSTEMCOMPUTER READABLE STORAGE MEDIUM IN WHICH INFORMATION PROCESSING PROGRAM OF CLIENT TERMINAL IS STOREDCOMPUTER READABLE STORAGE MEDIUM IN WHICH INFORMATION PROCESSING PROGRAM OF MANAGEMENT SERVER IS STOREDINFORMATION PROCESSING PROGRAM OF CLIENT TERMINALINFORMATION PROCESSING PROGRAM OF MANAGEMENT SERVERCOPY MANAGING METHODINFORMATION PROCESSING METHOD OF CLIENT TERMINAL AND INFORMATION PROCESSING METHOD OF MANAGING SERVER

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent unauthorized copy of the contents. SOLUTION: IDs (MIDs) are attached by every optical disk and the contents are encoded and recorded by a Content-Key. A system server manages a client ID of a client terminalan HDD-ID of an HDD and an MC-ID of a memory cardetc.owned by a user as user entry information. The user transmits the MC-ID to the system

server together with the MID of an optical disk when the contents are copied. The system server specifies the user by collating the MC-ID with the user entry information and returns the Content-Key used in the case of decoding the contents. The contents recorded in the optical disk is decoded and copied in the HDD by using the returned Content-Key on the user's side. Since copy of the contents is permitted only to a normal user as an owner of the storage mediumthe unauthorized copy of the contents is prevented.

---

## CLAIMS

---

[Claim(s)]

[Claim 1]A copy management system comprising:

A storage which contents enciphered with an enciphering key are memorizedand peculiar medium identification information is attached and is distributed to a user from the administrator side.

When it has a copy function which decrypts contents memorized by the above-mentioned storage using a decryption key corresponding to the above-mentioned enciphering keyand is copied to a secondary-storage medium and these contents are copiedwith medium identification information of the above-mentioned storage.

A terminal unit of a user who transmits predetermined and peculiar device identification information.

A management server device which transmits a decryption key of the above-mentioned contents to a terminal unit of a user who has the above-mentioned device identification information when a medium identification number of the above-mentioned storage is received.

[Claim 2]A copy management system which is the copy management system according to claim 1and is characterized by the above-mentioned management server device transmitting a decryption key once to one medium identification information.

[Claim 3]Are the copy management system according to claim 1 or 2and the above-mentioned terminal unitIdentification information of the above-mentioned terminal unitidentification information attached peculiar to a copy means which performs a copy of the above-mentioned contentsAnd a copy management system combining any one or plurality among identification numbers attached peculiar to external semiconductor memoryand transmitting as the above-mentioned device identification information.

[Claim 4]Are a copy management system given in any 1 paragraph among claim 1 to claims 3and the above-mentioned management server deviceA copy management system decrypting and using a decryption key which the above-mentioned decryption key is encipheredit transmits by the above-mentioned device identification informationand the above-mentioned terminal unit is the device identification information of selfand was enciphered [ above-mentioned ].

[Claim 5]A copy management system which is a copy management system given in any 1 paragraph among claim 1 to claims 4and is characterized by the above-mentioned terminal unit deleting the above-mentioned decryption key after decryption of the above-mentioned contents.
[Claim 6]Are a copy management system given in any 1 paragraph among claim 1 to claims 5and the above-mentioned management server deviceTransmit and a re-enciphering key for re-enciphering the above-mentioned contents which copy the above-mentioned terminal unitA copy management system decrypting contents copied [ above-mentioned ] and reproducing using a re-enciphering key which re-encipheredcopied contents decrypted with the above-mentioned decryption key with the above-mentioned re-enciphering keymemorized the above-mentioned re-enciphering key to a memory measureand was memorized to the above-mentioned memory measure.
[Claim 7]Are a copy management system given in any 1 paragraph among claim 1 to claims 6and the above-mentioned management server deviceDistribution management of the above-mentioned decryption key is performed by relatingmaking it each user's device identification informationand memorizing in a database medium identification information whose above-mentioned decryption key has been transmittedA copy management system rewriting old device identification information registered into the above-mentioned database to new device identification information when a user's device identification information is changed by repair or exchange.
[Claim 8]A copy management system which is a copy management system given in any 1 paragraph among claim 1 to claims 7and is characterized by the above-mentioned management server device performing predetermined accounting to a user who has the terminal unit which transmitted a decryption key.
[Claim 9]Are a copy management system given in any 1 paragraph among claim 1 to claims 8and mediate transmission and reception of information between the above-mentioned user's terminal unitand the above-mentioned management server deviceand. A copy management system having a mediation server device which performs accounting to a user when the above-mentioned decryption key is transmitted to a user's terminal unit at least.
[Claim 10]A storage characterized by comprising the following with which an information processing program of client terminal equipment was memorized and in which computer reading is possible.
A step which contents enciphered with an enciphering key are memorizedand reads this medium identification information from a storage to which peculiar medium identification information was given.
A step which reads device identification information attached peculiar to a device used when a user copies the above-mentioned contents.
a step which transmits medium identification information and device identification information which carried out [ above-mentioned ] reading appearance at least to a server apparatus by the side of an administrator.
A step which receives a decryption key replied from a server apparatus by the

side of the above-mentioned administrator by transmitting the above-mentioned medium identification information and device identification informationA step which carries out decoding processing of the contents memorized by the above-mentioned storage using a decryption key which received [ above-mentioned ]and a step which copies contents which carried out [ above-mentioned ] decoding processing.

[Claim 11]A step which is the storage according to claim 10 and receives the above-mentioned decryption keyA step which receives a decryption key enciphered and transmitted by device identification information of a user's deviceand carries out decoding processing of the above-mentioned contentsA storage carrying out decoding processing of the contents which carry out decoding processing of the decryption key enciphered [ above-mentioned ]and are memorized by the above-mentioned storage by device identification information of a self device using this decryption key that carried out decoding processing.
[Claim 12]A storage which is the storage according to claim 10 or 11and is characterized by having a step which deletes the above-mentioned decryption key after a copy of the above-mentioned contents.
[Claim 13]A storage given [ among claim 10 to claims 12 characterized by comprising the following ] in any 1 paragraph.
A step which receives a re-enciphering key for re-enciphering the above-mentioned contents which copy transmitted from the above-mentioned management server device.
A step which re-enciphers and copies contents decrypted with the above-mentioned decryption key with the above-mentioned re-enciphering key.
A step which memorizes the above-mentioned re-enciphering key to a memory measure.
A step which decrypts contents copied [ above-mentioned ] using a re-enciphering key memorized by the above-mentioned memory measure when reproducing contentsand is reproduced.

[Claim 14]In a step which is a storage given in any 1 paragraph among claim 10 to claims 13and transmits the above-mentioned medium identification information and device identification information. Identification information attached peculiar as this device identification information to a terminal unit which a user usesA storage transmitting one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copiedor identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.
[Claim 15]A storage characterized by comprising the following with which an information processing program of a management server device was memorized and in which computer reading is possible.
A step which receives device identification information which is transmitted from a

user's deviceand which was attached peculiar to this deviceand medium identification information attached peculiar to a storage with which contents enciphered with an enciphering key were memorized.
A step which detects whether medium identification information which received [ above-mentioned ] is registered into a database with which medium identification information of a storage with which a copy of contents was performed is registered in the state where it was related with device identification information of each user's device.
A step which transmits a decryption key for decrypting the above-mentioned contents to a user's device when un-registering of the above-mentioned device identification information is detected.

[Claim 16]A storage which is the storage according to claim 15 and is characterized by having a step which relates medium identification information to which the above-mentioned decryption key was transmitted with a device identification number of a device of a user who performed this transmissionand registers it into the above-mentioned database.
[Claim 17]A storage which it is the storage according to claim 15 or 16and a step which transmits the above-mentioned decryption key is the device identification information of a user's deviceand is characterized by enciphering the above-mentioned decryption key and transmitting.
[Claim 18]A storagewherein a step which is a storage given in any 1 paragraph among claim 15 to claims 17and transmits the above-mentioned decryption key transmits a re-enciphering key for re-enciphering the above-mentioned contents which copy.
[Claim 19]It is a storage given in any 1 paragraph among claim 15 to claims 18A storage having a step which rewrites old device identification information registered into the above-mentioned database to new device identification information when new device identification information is given by repair or exchange to a user's device.
[Claim 20]A storage which is a storage given in any 1 paragraph among claim 15 to claims 19and is characterized by having a step charged to a user who transmitted the above-mentioned decryption key.
[Claim 21]Are a storage of a statement given in any 1 paragraph among claim 15 to claims 20and in the above-mentioned medium identification information and a step which carries out device identification information reception. Identification information attached peculiar as this device identification information to a terminal unit which a user usesA storage receiving one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copiedor identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.
[Claim 22]An information processing program of client terminal equipment characterized by comprising the following.

A step which contents enciphered with an enciphering key are memorizedand reads this medium identification information from a storage to which peculiar medium identification information was given.
A step which reads device identification information attached peculiar to a device used when a user copies the above-mentioned contents.
a step which transmits medium identification information and device identification information which carried out [ above-mentioned ] reading appearance at least to a server apparatus by the side of an administrator.
A step which receives a decryption key replied from a server apparatus by the side of the above-mentioned administrator by transmitting the above-mentioned medium identification information and device identification informationA step which carries out decoding processing of the contents memorized by the above-mentioned storage using a decryption key which received [ above-mentioned ]and a step which copies contents which carried out [ above-mentioned ] decoding processing.

[Claim 23]A step which is the information processing program according to claim 22and receives the above-mentioned decryption keyA step which receives a decryption key enciphered and transmitted by device identification information of a user's deviceand carries out decoding processing of the above-mentioned contentsAn information processing program carrying out decoding processing of the contents which carry out decoding processing of the decryption key enciphered [ above-mentioned ]and are memorized by the above-mentioned storage by device identification information of a self device using this decryption key that carried out decoding processing.
[Claim 24]An information processing program which is the information processing program according to claim 22 or 23and is characterized by having a step which deletes the above-mentioned decryption key after a copy of the above-mentioned contents.
[Claim 25]An information processing program given [ among claim 22 to claims 24 characterized by comprising the following ] in any 1 paragraph.
A step which receives a re-enciphering key for re-enciphering the above-mentioned contents which copy transmitted from the above-mentioned management server device.
A step which re-enciphers and copies contents decrypted with the above-mentioned decryption key with the above-mentioned re-enciphering key.
A step which memorizes the above-mentioned re-enciphering key to a memory measure.
A step which decrypts contents copied [ above-mentioned ] using a re-enciphering key memorized by the above-mentioned memory measure when reproducing contentsand is reproduced.

[Claim 26]In a step which is an information processing program given in any 1 paragraph among claim 22 to claims 25and transmits the above-mentioned medium

identification information and device identification information. Identification information attached peculiar as this device identification information to a terminal unit which a user usesAn information processing program transmitting one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copiedor identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.
[Claim 27]An information processing program of a management server device characterized by comprising the following.
A step which receives device identification information which is transmitted from a user's deviceand which was attached peculiar to this deviceand medium identification information attached peculiar to a storage with which contents enciphered with an enciphering key were memorized.
A step which detects whether medium identification information which received [ above-mentioned ] is registered into a database with which medium identification information of a storage with which a copy of contents was performed is registered in the state where it was related with device identification information of each user's device.
A step which transmits a decryption key for decrypting the above-mentioned contents to a user's device when un-registering of the above-mentioned device identification information is detected.

[Claim 28]An information processing program which is the information processing program according to claim 27and is characterized by having a step which relates medium identification information to which the above-mentioned decryption key was transmitted with a device identification number of a device of a user who performed this transmissionand registers it into the above-mentioned database.
[Claim 29]An information processing program which it is the information processing program according to claim 27 or 28and a step which transmits the above-mentioned decryption key is the device identification information of a user's deviceand is characterized by enciphering the above-mentioned decryption key and transmitting.
[Claim 30]An information processing programwherein a step which is an information processing program given in any 1 paragraph among claim 27 to claims 29and transmits the above-mentioned decryption key transmits a re-enciphering key for re-enciphering the above-mentioned contents which copy.
[Claim 31]It is an information processing program given in any 1 paragraph among claim 27 to claims 30An information processing program having a step which rewrites old device identification information registered into the above-mentioned database to new device identification information when new device identification information is given by repair or exchange to a user's device.
[Claim 32]An information processing program which is an information processing program given in any 1 paragraph among claim 27 to claims 31and is characterized

by having a step charged to a user who transmitted the above-mentioned decryption key.
[Claim 33]Are an information processing program of a statement given in any 1 paragraph among claim 27 to claims 32and in the above-mentioned medium identification information and a step which carries out device identification information reception. Identification information attached peculiar as this device identification information to a terminal unit which a user usesAn information processing program receiving one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copiedor identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.
[Claim 34]When copying contents enciphered and memorized with an enciphering key with a user's device to which a peculiar device identification number was given by storage to which peculiar medium identification information was givenThe above-mentioned device identification information and the above-mentioned medium identification information are transmitted to a management server device from the above-mentioned deviceMedium identification information of a storage with which a copy of contents was performed in a database registered in the state where it was related with device identification information of each user's device. The above-mentioned management server device detects whether medium identification information transmitted from the above-mentioned user's device is registeredA copy management method which transmits a decryption key for decrypting the above-mentioned contents from the above-mentioned management server device to a user's device to the above-mentioned database when the above-mentioned medium identification information is unregistered.
[Claim 35]Contents enciphered with an enciphering key are memorizedand from a storage to which peculiar medium identification information was given. Read this medium identification information and device identification information attached peculiar to a device used when a user copies the above-mentioned contents is readby transmitting medium identification information and device identification information which carried out [ above-mentioned ] reading appearance at least to a server apparatus by the side of an administratorand transmitting the above-mentioned medium identification information and device identification information.An information processing method of client terminal equipment which carries out decoding processing of the contents which receive a decryption key replied from a server apparatus by the side of the above-mentioned administratorand are memorized by the above-mentioned storage using a decryption key which received [ above-mentioned ]and copies contents which carried out [ above-mentioned ] decoding processing.
[Claim 36]Device identification information which is transmitted from a user's device and which was attached peculiar to this deviceIn and the state where received medium identification information attached peculiar to a storage with which contents enciphered with an enciphering key were memorizedand it was

related with device identification information of each user's device. In a database with which medium identification information of a storage with which a copy of contents was performed is registered. An information processing method of a management server device which transmits a decryption key for decrypting the above-mentioned contents to a user's device when it detects whether medium identification information which received [ above-mentioned ] is registered and un-registering of the above-mentioned device identification information is detected.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This inventionFor examplethe storage with which the information processing program of a copy management system and client terminal equipment which performs copy management of computer programssuch as game contentsmovie contentsa music contentand an application programwas memorized and in which computer reading is possibleThe information processing program of the storage with which the information processing program of the management server device was memorized and in which computer reading is possibleand client terminal equipmentan information processing program of a management server devicea copy management methodan information processing method of client terminal equipmentAnd it is related with the information processing method of a management server device.
[0002]
[Description of the Prior Art]In todaythe video game machine which performs a video game based on the game contents memorized by storagessuch as CD-ROMDVD-ROMor semiconductor memoryhas spread widely.
[0003]A user purchases the storage with which desired game contents were memorizedreproduces this storage with a video game machineand performs a video game. When the mostthe user buys and arranges a new video game gradually. For this reasonthe storage with which each game contents were memorized will be accumulated to the user with days and months.
[0004]Howeverone reproducing mechanism of a storage is provided in the video game machine in many cases. For this reasonwhen a different video game was performedthe storage with which the video game machine is equipped now was taken outand very troublesome work [ say / newly reequipping with the storage with which the game contents which it will try to perform from now on were memorized ] was needed.
[0005]
[Problem(s) to be Solved by the Invention]This applicant is indicating the video game machine which made possible built-in or external [ of the mass hard disk drive (HDD) of tens of OrderG (G) ]for example.

[0006]In the case of this video game machinethe game contents memorized by each storage can be copied to HDDrespectivelyand desired game contents can be reproduced and used from this HDD. By using this HDDthe time and effort which detaches and attaches a storage to the reproducing mechanism of a video game machine is omissible.
[0007]Only the user who computer programssuch as game contentspurchased here software with which the computer program was memorizedand received justly is usable ****.
[0008]Howeverwhen the copy of the computer program memorized by the storage is enabled at a secondary-storage mediumwe are anxious about the illegal copy which uses the computer program memorized by one storage for a secondary-storage medium in two or more users copying itrespectively.
[0009]It is this invention's being made in view of an above-mentioned technical problemand performing copy management which enables the copy of a computer program only to a valid userPrevention of an unauthorized use of contentsetc. A storage with which the information processing program of the copy management system and client terminal equipment which were planned was memorized and in which computer reading is possiblea storage with which the information processing program of the management server device was memorized and in which computer reading is possiblean information processing program of client terminal equipmentIt aims at offer of the information processing program of a management server devicea copy management methodthe information processing method of client terminal equipmentand the information processing method of a management server device.
[0010]
[Means for Solving the Problem]This invention attaches a peculiar identification number to a storage which made contents enciphered with an enciphering key memorizeand distributes it to a user. An identification number is given also to a device used when a user copies contents.
[0011]When the above-mentioned device copies contentsit transmits an identification number of the above-mentioned storageand an identification number of a device to a management server device. A management server device has the database with which an identification number of a device which each user uses was registered. A management server device compares an identification number of a device registered into a databaseand an identification number of a device transmitted from a user's deviceand specifies a user. A management server device transmits a decryption key for decrypting contents memorized by storage to a user's devicewhen a user is specified by performing this collation.
[0012]A user's device decrypts contents memorized by the above-mentioned storage based on a decryption key distributed from this administrator sideand copies contents.
[0013]A copy of contents can be permitted by this only to a regular user who is an owner of a storageand an illegal copy of contents can be prevented.
[0014]

[Embodiment of the Invention]This invention is applicable to the copy management system which performs copy management of a computer program.
[0015]As a computer programthere are game contentsa music contentmovie contentsan application programetc.for example. As a storage with which the computer program was memorizedthere is semiconductor memory besides optical discssuch as DVD-ROM and CD-ROM. As a secondary-storage medium used as the copy destination of a computer programthere are a hard disk (HD)DVD-RAMa magneto-optical disc (MO)etc.
[0016]Hereafterthe above-mentioned game contentsa music contentmovie contentsan application programetc. are named genericallyand it is only considered as "contents."
[0017][Entire configuration of a copy management system] The entire configuration of the copy management system used as a 1st embodiment of this invention is first shown in drawing 1. As shown in this drawing 1the copy management system of this 1st embodiment has the client terminal equipment 1 provided with the regenerative function (execution function) of the contents memorized by the optical discand the communication function through a network.
[0018]The hard disk drive 2 (HDD) for copying the contents memorized by the optical disc is connected to this client terminal equipment 1.
[0019]Communication MODEM 6 for aiming at connection with networkssuch as the Internet 5is connected to this client terminal equipment 1.
[0020]Communication MODEM 6 may be formed in an external form to the client terminal equipment 1as shown in this drawing 1. Communication MODEM 6 may be formed in the form of built-in in the client terminal equipment 1.
[0021]The copy management system has the system server device 4 provided with the database 3 with which user entry information was memorized.
[0022]The copy management system of this 1st embodiment comprises that this system server device 4 and the above-mentioned client terminal equipment 1 are mutually connectedfor example via the network of Internet 5 grade.
[0023][Composition of client terminal equipment] The perspective view of the appearance of the client terminal equipment 1 is shown in drawing 2. this -- the controller terminal areas 7A and 7B and the memory card applied parts 8A and 8B are formed in the front-face side of the client terminal equipment 1 so that it may be shown figure 2.
[0024]To the front-face side of this client terminal equipment 1. The two USB contact buttons 9 to which the apparatus (USB:Universal Serial Bus) corresponding to USB is connectedand the IEEE1394 contact button 10 which can respondfor example to the data transfer rate of a maximum of 400 Mbps(es) are formed.
[0025]The disk applied part 11 of the tray mold with which it is equipped with an optical disc is formed in the front-face side of this client terminal equipment 1.
[0026]The reset button 12 for resetting execution operation and reproduction motion of contents and the tray manual operation button 13 for operating receipts and payments of the tray of the optical disc applied part 11 are formed in the

front-face side of this client terminal equipment 1.
[0027]An electric power switchthe voice image output terminal (AV multi output terminal)the PC Card slotthe optical digital output terminalthe AC power input terminaletc. are provided in the back side of the client terminal equipment 1.
[0028]AV multi output terminal is connected to the television receiver 18 for a monitor via the AV cable 17. The video signal and audio signal which are outputted from the client terminal equipment 1 are supplied to the television receiver 18 for a monitor via this AV multi output terminal and the AV cable 17. Therebythe image of the above-mentioned contents is displayed on the television receiver 18. The sound of the above-mentioned contents is pronounced via the loudspeaker device of a television receiver.
[0029]The controller 14 is connected to the controller terminal areas 7A and 7B via the controller cable 15respectively.
[0030]The memory card applied parts 8A and 8B are equipped with the memory card for a save etc. which perform a save (memory) and read-out of game data.
[0031][Composition of a hard disk drive] Nextin drawing 2the case currently laid in the upper face part of the client terminal equipment 1 is the hard disk drive 2 (henceforth HDD2). This HDD2large hard diskssuch as 40 GBare provided in the inside. The game contents memorized by DVD-ROM for about ten sheets can be copied to this HDD2.
[0032]The power indicator 20 by which a lighting drive is carried outand the write-in indicator lamp 21 by which a lighting drive is carried out by being interlocked with the writing to a hard disk are formed in the power up at the front-face side of HDD2. The electric power switch and the data input/output terminal are provided in the back side of HDD2 at least.
[0033]A PC card is inserted in the above-mentioned PC Card slot provided in the back side of the client terminal equipment 1 when connecting HDD2 to the client terminal equipment 1. The end of a connecting cable is connected to a PC card in this state. The other end of a connecting cable is connected to the data input/output terminal of HDD2. Therebythe client terminal equipment 1 and HDD2 are electrically connected mutually.
[0034]In this exampleHDD2 is a different body in the client terminal equipment 1and we decided to carry out external to the client terminal equipment 1. Howeverthis HDD2 may be provided in the form built in the client terminal equipment 1.
[0035]It was presupposed that the client terminal equipment 1 and HDD2 are connected with a PC card via a connecting cable. Howevercontact buttonssuch as a USB contact button and an IEEE1394 contact buttonare provided in the back side (or it may be a front-face side.) of HDD2and it may be made to connect HDD2 to the client terminal equipment 1 via this contact button.
[0036][Electric constitution of client terminal equipment] Nextdrawing 3 is a block diagram of the client terminal equipment 1. As shown in this drawing 3the client terminal equipment 1 has CPU30the graphic processor 31 (GPU)and IO processor 32 (IOP).

[0037]The client terminal equipment 1 is provided with the following.
The optical-disc-controlling part 33 which performs reproduction control of optical discssuch as CD-ROM and DVD-ROM.
Sound processor unit 34 (SPU).

[0038]The client terminal equipment 1 is provided with the following.
MASK-ROM35 in which the operating system program which CPU30 and IOP32 execute was stored.
RAM36 which functions as a buffer which stores temporarily the data read from the work area and optical disc of CPU30.

[0039]The client terminal equipment 1 has CD/DVDDSP38 which performs and outputs error correction processing (CIRC processing) etc. as opposed to the reproducing output from the optical disc supplied via RF amplifier 37 of the optical-disc-controlling part 33.
[0040]The client terminal equipment 1 has the driver 39 and the mechanical-completion troller 40 which perform the roll control of the spindle motor of the optical-disc-controlling part 33the focus/tracking control of an optical pickuploading control of a disk trayetc.
[0041]The client terminal equipment 1 has the card shape connector 41 to which the above-mentioned PC card is connected.
[0042]These each part is mainly mutually connected via the bus line 42 and 43 gradesrespectively.
[0043]Reproduction of the movie contents memorized by DVD-ROM is performed based on the DVD driver SOUFUTO wear memorized by the memory card. Or reproduction of movie contents is performed based on the DVD driver SOUFUTO wear printed on the semiconductor memory 44 (DVD Player ROM) built in in the client terminal equipment 1.
[0044]The operating system program is memorized by MASK-ROM35. CPU30 controls operation of the client-terminal-equipment 1 whole based on the operating system program memorized by this MASK-ROM35.
[0045]The hardware identification number (hardware ID) of the controller terminal areas 7A and 7Bthe memory card applied parts 8A and 8B and the controller 14 connected to the card shape connector 41the memory card 16and the HDD2 grade is also memorized by MASK-ROM35. Based on hardware ID memorized by this MASK-ROM35IOP32It communicates with the hardware of the controller 14the memory card 16and HDD2 gradeand the hardware connected to each contact buttons 7A7B8Aand 8B and card shape connector 41 grade is specified and recognized.
[0046]Hardware ID means ID generically attached to each hardware so to speak like one ID by one ID and the memory card 16 whole by the client-terminal-equipment 1 whole at one ID and the HDD2 whole.
[0047]On the other handclient IDMC-IDand HDD-ID which are mentioned later are every client terminal equipmentevery memory card 16and ID peculiar to each

hardware attached for every HDD2respectively.
[0048]GPU31 is stored in the frame buffer which draws according to the drawing indication from CPU30and does not illustrate the drawn picture. GPU31 has a function as a geometry transfer engine which processes coordinate conversion etc.
[0049]This GPU31 constitutes a virtual three-dimensional object from a set of the polygon of triangular shapewhen the game contents currently recordedfor example on the optical disc use what is called 3D graphics. And GPU31 performs many calculations for generating the picture acquired by photoing this three-dimensional object with a virtual camera device. That isGPU31 performs transparent transformation processing in the case of performing a rendering (calculation of the coordinate value at the time of projecting the peak of each polygon which constitutes a three-dimensional object on a virtual camera screen)etc.
[0050]GPU31 draws to a frame bufferusing a geometry transfer engine if needed according to the drawing indication from CPU30. And the video signal (visual out) corresponding to this picture that drew is outputted.
[0051]On the other handSPU34 is reproducing the data point remembered to be the ADPCM function decoding which reproduces the voice data by which adaptive predictive coding was carried out by the sound bufferIt has the regenerative function which reproduces and outputs audio signalssuch as a sound effect (audio out)the abnormal-conditions function which is made to modulate the data point memorized by the sound bufferand is reproducedetc. This SPU34 operates as what is called a source of a sampling sound. SPU34 generates audio signalssuch as musical tone and a sound effectbased on the data point memorized by ** Li and the sound buffer from CPU30 to directions.
[0052]As for such client terminal equipment 1if a power supply is switched onCPU30 and IOP32 will read the operating system program for CPU30and the operating system program for IOP32 from MASK-ROM35respectively.
[0053]CPU30 controls each part of the client terminal equipment 1 by the operating system program for CPU30 in generalization. IOP32 controls input and output of the data between the controller 14the memory card 16and HDD2 grade by the operating system program for IOP32.
[0054]After CPU30 performs initialization processingssuch as operation confirmingbased on the operating system program for CPU30it controls the optical-disc-controlling part 33and carries out reproduction control of the contents currently recorded on the optical disc.
[0055]When the reproduced contents are game contents of a video gameCPU30According to the directions (command) from the player received from the controller 14 via IOP32GPU31 and SPU34 are controlled and utterance of the display of the picture of game contentsa sound effectmusical toneetc.etc. is controlled.
[0056]When the reproduced contents are movie contentsaccording to the directions from the player received from the controller 14 via IOP32CPU30 controls GPU31 and SPU34 and controls the display of the image of movie contentsaudio utteranceetc.

[0057][Copy management activities] Such a copy management system is managed as followswhen the contents memorized by the optical disc are copied to HDD2.
[0058][Installation of an installer] Firstwhen this copy management system copies the contents memorized by the optical disc to HDD2it needs to execute the application program for copy control (installer) with the client terminal equipment 1. In the case of this examplethe installer is memorized by the optical disc with contents. The client terminal equipment 1 installs an installer before copy **** of contents.
[0059]When installing an installera user equips the client terminal equipment 1 with the optical disc in which the installer is memorized. If equipped with this optical discCPU30 of the client terminal equipment 1 will read the installer memorized by the optical disc according to operation of a user's controller 14 automatically (auto run)and will carry out storage control of this to memory card 16 or RAM36.
[0060]The installer memorized by this memory card 16 or RAM36 is performed by CPU30 when a user specifies the copy of the contents memorized by the optical disc. CPU30 is performing this installer and performs copy control of contents.
[0061]An installer manufactures the optical disc in which only the installer was memorized by the system contractor sideand it may be made to distribute this to a user. Or the memory card in which the installer was memorized by the system contractor side is manufacturedand it may be made to distribute this to a user. In this caseinstall work of an installer can be made omissible.
[0062]Or ROM the installer was remembered to be may be provided in the client terminal equipment 1. Even in this caseinstall work of an installer can be made omissible.
[0063][Encryption of contents] Encryption processing is performed to the contents memorized by the optical disc using a symmetrical key (contents key: Content-Key) which is different for every contents as shown in drawing 4. "Media unique ID (media unique ID:MID)" which becomes peculiar for every optical disc besides the contents by which encryption processing was carried out in this way is memorized by the optical disc.
[0064][User registration] Nextin the copy management system of this 1st embodimentwhen copying contents to HDD2 from an optical discit registers for the system server device 4 as a user using "memory card ID (MC-ID)" given to each memory card 16 peculiar. The copy of contents is not permitted when this user registration is not performed.
[0065]Drawing 5 is a flow chart which shows a flow until a user registers as a user to the system server device 4. Drawing 6 is a mimetic diagram of the copy management system concerned in which the information transmitted and received by this user registration between the client terminal equipment 1 and the system server device 4 is shown.
[0066]User registration operation is explained using this drawing 5 and drawing 6. The flow chart of drawing 5 is started because a user switches on the main power of the client terminal equipment 1.
[0067]In Step S1a user connects his own client terminal equipment 1 to the

system server device 4 via the Internet 5.
[0068]As shown in drawing 1specificallycommunication MODEM 6 for Internet connectivities is connected to this client terminal equipment 1 (or built-in). If an Internet connectivity is specified by the userCPU30 shown in drawing 3 will operate based on a predetermined WWW browserand will aim at establishment of the communication line between the client terminal equipment 1 concerned and the system server device 4 via this communication MODEM 6. Therebythe distance of this user registration progresses to Step S2.
[0069]The identification number (MC-ID) of the memory card in which the client terminal equipment 1 was equipped with CPU30 in Step S2The transmission control of the peculiar identification number (HDD-ID) attached for every peculiar identification number (client ID) attached for every client terminal equipment and HDD2 is carried out to the system server device 4.
[0070]If the communication line of the system server device 4 and the client terminal equipment 1 is establishedspecificallyCPU30 will communicate with the client terminal equipment 1HDD2and the memory card 16respectively. The identification number with which CPU30 was given to the client terminal equipment 1 by this communication peculiar (client ID)The identification number (HDD-ID) attached peculiar to HDD2 and the identification number (MC-ID) given to the memory card 16 with which the client terminal equipment 1 was equipped peculiar are acquiredrespectively.
[0071]CPU30 transmits these identification numbers to the system server device 4 sideas shown in drawing 6. Therebythe distance of this user registration progresses to Step S3.
[0072]Information is encipheredtransmitted and receivedfor example based on communications protocolssuch as SSL (Secure Sockets Layer)and communicative safety is secured between the client terminal equipment 1 and the system server device 4.
[0073]In this exampleCPU30 is communicating with each device and decided to acquire client IDHDD-IDand MC-IDand to transmit to the system server device 4 side. Howeverthe user is stuck on the client terminal equipment 1HDD2and the memory card 16 for client IDHDD-IDand MC-ID in the ability to be recognized visually at each caserespectively. For this reasonthis client IDHDD-IDand MC-ID are seenand a user operates the controller 14inputs each ID manuallyand may be made to transmit to the system server device 4 side.
[0074]Nextin Step S3the identification number (MC-ID) of the memory card in which the system server device 4 was transmitted by this user distinguishes whether it is effective ID. In this step S3this user registration distance progresses to step S4when MC-ID to which the system server device 4 was transmitted by the user distinguishes that it is effective IDand when it distinguishes that MC-ID transmitted by the user is invalid IDit progresses to Step S7.
[0075]Specificallythe system server device 4 has the database 3 which memorized client ID of all the client terminal equipment 1HDD-ID of all the HDD2and MC-ID of all the memory cards 16.

[0076]the system server device 4 -- the client terminal equipment 1 from a userHDD2and the memory card 16 -- eachif peculiar ID is transmittedFirstMC-ID which is peculiar ID of the memory card 16 transmitted by the userand each MC-ID registered into the database 3 are comparedand it is distinguished whether the same MC-ID as MC-ID of the memory card 16 transmitted by the user is registered into the database 3.
[0077]That isthe system server device 4 distinguishes whether MC-ID of the memory card 16 transmitted by the user is the same as MC-ID regularly registered into the database 3.
[0078]When MC-ID of the memory card 16 transmitted by the user is in agreement with neither of MC-ID regularly registered into the database 3as for the system server device 4access of this user registration is judged to be access of unjust user registration. In this casethe system server device 4 replies the message which refuses user registration of "being unable to register as a user in this memory card" to the client-terminal-equipment 1 side in Step S7 (invalid notice). By thisthis user registration distance will be completed in the form where user registration was interrupted.
[0079]When MC-ID of the memory card 16 transmitted by the user is in agreement with one which is regularly registered into the database 3 of MC-IDon the other handthe system server device 4In step S4the user ID (User ID) which is peculiar ID of the user who has accessed the system server device 4 is formed nowfor example using a random number etc.
[0080]And as shown in drawing 6the system server device 4 with the user's client IDHDD-IDand MC-ID. The user ID (User ID) which is the above-mentioned user's peculiar IDand MC-Key explained later are put togetherand it registers with the database 3 of the system server device 4 by making this into "user entry information."
[0081]Thusthe copy management system of the embodiment concerned specifies each user in the combination of three IDthe client terminal equipment 1 which each user ownsHDD2and the memory card 16and registers him into the database 3.
[0082]Since it is not possibleit can register by registering as a user based on these three ID that the client terminal equipment 1HDD2and three ID of the memory card 16 are altogether in agreement among different users as a user by certainly specifying a user. The illegal copy of the contents recorded on the optical disc mentioned later by this can be prevented more powerfully.
[0083]In the case of user registrationonly "MC-ID" and "client ID"It may be made to register as a user by transmitting "HDD-ID"MC-ID and client IDMC-ID and HDD-IDor "client ID and HDD-ID" to the system server device 4 side. not overlapping among different users in these casessince each ID is peculiar IDrespectively -- a user -- abbreviated ** -- it can register as a user by certainly specifying.
[0084]Nextwhen the distance of user registration progresses to Step S5the system server device 4As a proof which user registration completed regularlyuser

ID (User ID) is enciphered by MC-Key among the user entry information formed by the above-mentioned step S4and this is replied to the client-terminal-equipment 1 side.
[0085][MC-Key] Herethe above "MC-Key" is the key information for enciphering the information transmitted and received between the client terminal equipment 1 and the system server device 4. This MC-Key is beforehand memorized in the memory card 16 with MC-ID.
[0086]It is stuck on the case of the memory card 16 so that a user can recognize MC-ID visuallybut it is remembered in the memory card 16 that a user cannot recognize this MC-Key visually. This MC-Key has been the high information on confidentiality that neither a display nor an output is performedeven when a user reproduces the information memorized in the memory card 16. For this reasonthis MC-Key cannot be recognized by user levels.
[0087]MC-Key memorized by each memory card 16 with MC-ID of all the memory cards 16 is memorized by the database 3 of the system server device 4. When MC-Key is neededread and refer to MC-Key for the system server device 4 from this database 3. For this reasonMC-Key is not transmitted from the client terminal equipment 1 to the system server device 4.
[0088]ThusMC-Key has been the high information on confidentiality which cannot recognizeand is not transmitted and received between the client terminal equipment 1 and the system server device 4 in user levels.
[0089]By making unnecessary transmission and reception of MC-Key between the client terminal equipment 1 and the system server device 4MC-Key can prevent the inconvenience monitored by the third party.
[0090]When the system server device 4 replies user ID (User ID)it chooses MC-Key corresponding to a user's memory card 16 accessed now from MC-Key beforehand memorized by the database 3. And user ID (User ID) is enciphered using this selected MC-Keyand it replies to the client terminal equipment 1.
[0091]This MC-Key is used when decrypting the above-mentioned user ID (User ID)media unique ID (media unique ID (MID))a contents key (Content-Key)and Content-Gen-Keyrespectively.
[0092]MID is ID attached peculiar for every optical disc. A contents key is the encryption key used when carrying out encryption processing of the contents recorded on the optical disc. Content-Gen-Key is an encryption key used when performing re-encryption processing to the contents copied to HDD2.
[0093]The client terminal equipment 1 decrypts the contents played from the optical disc using the above-mentioned contents key. And the client terminal equipment 1 carries out re-encryption processing using above-mentioned Content-Gen-Keyand copies these decrypted contents to HDD2. It mentions later in detail.
[0094]Nextif user registration distance progresses to Step S6the client terminal equipment 1 will carry out storage control of the user ID (User ID) replied from the system server device 4 side to the memory card 16. Therebythe complete process cycle of the user registration shown in the flow chart of this drawing 5 is

completed. And at this timethe user ID (User ID) enciphered by MC-Key with MC-ID and MC-Key which are beforehand memorized as shown in drawing 6 will be memorized by the memory card 16.
[0095][Registration of media unique IDand acquisition of a contents key] Nextonly by lending the memory card 16 in which MC-IDMC-Keyand user ID (User ID) were recorded to other usersif the copy of the contents currently recorded on the optical disc is enabled any number of times HDD2It becomes possible to copy unjustly the contents currently recorded on the optical disc to other users' HDDand other users are not desirable thingseither.
[0096]When copying contents to HDD2 in the case of this copy management systema user transmits peculiar media unique ID (media unique ID (MID)) attached for every optical disc via the client terminal equipment 1 to the system server device 4 side. The system server device 4 registers media unique ID transmitted by the userand it transmits the contents key for decrypting the enciphered contents to a user. The client terminal equipment 1 decrypts the contents currently recorded on the optical disc using a contents keyand copies them to HDD2. For this reasonreceiving this contents key means that the copy of contents was permitted from the system server device 4 to the client terminal equipment 1.
[0097]The system server device 4 transmits a contents keyafter checking that transmission of the contents key had not been performed in the past to media unique ID which received from the client terminal equipment 1. Therebytransmission of the contents key to the same media unique ID can be restricted only at once.
[0098]For exampleafter a certain user copies the contents memorized by the optical disc purchased by itself to his HDD2suppose that this optical disc was lent to other users. When other users copy contents to HDD2they transmit media unique ID of the lent optical disc to the system server device 4.
[0099]Howeverthe history which shows that transmission of the contents key was performed remains in the system server device 4 side to media unique ID of the optical disc. In this casedistribution of a contents key does not perform the system server device 4 to other users. Other users who cannot obtain a contents key cannot copy contents to HDD2. This copy management system was carried out in this wayand has prevented the illegal copy of contents.
[0100]A flow until registration and the user of media unique ID (MID) acquire a contents key to the flow chart of drawing 7 is shown. Each information transmitted and received between the client terminal equipment 1 and the system server device 4 in the case of acquisition of a contents key in the case of the registration of media unique ID to drawing 8 is shown.
[0101]Registration of media unique ID (MID) and the acquisition operation of a contents key are explained using this drawing 7 and drawing 8. The registration of media unique ID (MID) and the acquisition distance (registration acquisition distance) of a contents key which are shown in the flow chart of this drawing 7 are performed [ that the user is terminating the above-mentioned user registration regularly and ] as a premise.

[0102]Firstin Step S11the client terminal equipment 1 aims at establishment of the communication line between the system server devices 4. Therebythis registration acquisition distance progresses to Step S12.
[0103]In this examplethe communication line established between the client terminal equipment 1 and the system server device 4 after the above-mentioned end of user registration is once cutAt the time of execution of this registration acquisition distanceit is the explanation which establishes the communication line between the client terminal equipment 1 and the system server device 4 again.
[0104]Howeverit may be made to perform this registration acquisition distancewithout cutting the communication line established between the client terminal equipment 1 and the system server device 4 after the above-mentioned user registration. In this casethis registration acquisition distance will skip Step S11and will progress to Step S12 from a start.
[0105]Nextin Step S12the client terminal equipment 1 transmits the user ID (User ID) and MC-ID which were acquired as mentioned above to the system server device 4. The client terminal equipment 1 transmits media unique ID (MID) attached peculiar with this user ID and MC-ID to the optical disc in which the contents to be copied to HDD2 from now on were memorized to the system server device 4 side.
[0106]CPU30 communicates with the memory card 16and as shown in drawing 8specificallyit transmits MC-ID to the system server device 4 side. CPU30 reads the user ID enciphered by MC-Key as mentioned above from the memory card 16and transmits to the system server device 4 side. CPU30 enciphers media unique ID (MID) which controlled the optical-disc-controlling part 33 and was played from the optical disc by MC-Keyand transmits this to the system server device 4 side.
[0107]It may be made to transmit client ID and HDD-ID to the system server device 4 side with each of these information. Client ID and HDD-ID can be used for a user's specification with above-mentioned MC-ID. A user can be specified more correctly than the case where a user is specified only by MC-IDby specifying a user using three IDMC-IDclient IDand HDD-ID.
[0108]The information transmitted and received between the client terminal equipment 1 and the system server device 4 is encipheredtransmitted and receivedfor example based on communications protocolssuch as SSL (Secure Sockets Layer). Therebyhigh communication of safety can be performed between the client terminal equipment 1 and the system server device 4.
[0109]Nextin Step S13the user ID (User ID) to which the system server device 4 was transmitted from the client-terminal-equipment 1 side distinguishes whether it is effective ID. In this step S13when the system server device 4 distinguishes that user ID is effectivethis registration acquisition distance progresses to Step S14. On the other handin this step S13when the system server device 4 distinguishes that user ID is invalidthis registration acquisition distance progresses to Step S17.
[0110]Specificallythe system server device 4 reads MC-Key corresponding to this

MC-ID with reference to the database 3 based on MC-ID (and client IDHDD-ID) transmitted from the client-terminal-equipment 1 side. And the system server device 4 decrypts the user ID (User ID) and media unique ID (MID) which were enciphered and transmitted by MC-Key based on this MC-Keyrespectively.
[0111]As mentioned aboveuser ID (User ID)MC-IDclient IDHDD-IDetc. are memorized as user entry information by the database 3 by the side of the system server device 4. For this reasonthe system server device 4 searches User Information in the database 3 based on MC-ID (client ID and HDD-ID). And the system server device 4 compares the user ID (User ID) within this User Informationand the user ID (User ID) of the user who is accessing the present system server device 4 side. The system server device 4 judges the user who is accessing the present system server device 4 side to be a regular userwhen above-mentioned both are in agreement. Therebythis registration acquisition distance progresses to Step S14.
[0112]The system server device 4 On the other handthe user ID (User ID) within User Information of the database 3When the user ID (User ID) of the user who is accessing the present system server device 4 side is inharmoniousit is judged that the user ID (User ID) is invalid. And the system server device 4 has [ in / Step S17 ] invalid "user ID. Please register as a user. The message which stimulates user registration of " etc. for the second time is replied to the client-terminal-equipment 1 side (invalid notice). This will be completed in the form where this registration acquisition distance was interrupted.
[0113]Nextin Step S14the contents currently recorded on the user's optical disc which the system server device 4 is accessing now distinguish whether there is any history copied in the past.
[0114]Specificallyin the case of this copy management systemall media unique ID (MID) given to each optical discrespectively is registered into the database 3. The system server device 4 leaves the history of a copy by setting a flag to media unique ID (MID) of the database 3when the copy of contents is performed.
[0115]For this reasonthe system server device 4 will detect whether the flag stands to that media unique ID (MID)if media unique ID (MID) is decrypted. Therebyit can be distinguished whether the copy of contents was performed in the past from the optical disc which has the media unique ID (MID).
[0116]When the flag of the media unique ID (MID) does not standit means that the copy of contents is not performed in the past from the optical disc to which the media unique ID (MID) was given. For this reasonthe system server device 4 sets the flag of that media unique ID (MID) in the database 3. The system server device 4 registers into that user's user entry information media unique ID (MID) which set this flagand advances this registration acquisition distance to Step S15.
[0117]On the other handwhen the flag of the media unique ID (MID) standsit means that the copy of contents is performed from the optical disc to which the media unique ID (MID) was given in the past. For this reasonthe system server device 4 replies the message which refuses the copy of the contents of "being unable to copy contents from these media" to the client-terminal-equipment 1

side in Step S17 (invalid notice). This will be completed in the form where this registration acquisition distance was interrupted.
[0118]NextStep S15 is a step which progresses when the copy of contents is not performed from the user's optical disc in the past. In this casethe system server device 4 enciphers the contents key (Content-Key) which enciphered the contents currently recorded on the optical disc using MC-Key of that user's memory card 16. And this enciphered contents key is transmitted to the client-terminal-equipment 1 side. Transmission of this contents key means that the copy of the contents currently recorded on the optical disc from the system server device 4 side to the user was permitted.
[0119]MC-Key is attached peculiar to the memory card 16 which the user owns. For this reasonit can limit only to the user who has the memory card 16 in which that MC-Key was memorized in the user who can decrypt and use this contents key. Thereforethe above-mentioned contents key can be safely transmitted only to a regular user.
[0120]The system server device 4 reads HDD-ID of the clients ID and HDD2 of the client terminal equipment 1 which the user is using based on the user entry information memorized by the database 3. It enciphers by "contents JIENKI (Content-Gen-Key)" which formed these each IDfor example using the random numberand the system server device 4 is replied to the client-terminal-equipment 1 side.
[0121]The system server device 4 enciphers by above-mentioned MC-Keyand replies contents JIENKI (Content-Gen-Key) used when enciphering client ID and HDD-ID to the client-terminal-equipment 1 side.
[0122]Although explained laterthe client terminal equipment 1 compares client ID replied from the system server device 4and client ID of the client terminal equipment 1 concerned. The client terminal equipment 1 compares HDD-ID transmitted from the system server device 4and HDD-ID of HDD2 connected to the client terminal equipment 1 concerned. And two above-mentioned client ID and two above-mentioned HDD-ID check that it is in agreementrespectivelyand the client terminal equipment 1 copies contents.
[0123]For this reasonby replying client ID and HDD-ID which are beforehand registered from the system server device 4 to a user's client terminal equipment 1The copy of contents can be enabled only in the user's client terminal equipment 1 and the combination of HDD2 which are beforehand registered into the database 3.
[0124]The system server device 4 enciphers contents JIENKI which enciphered client ID and HDD-ID using MC-Key given to the memory card 16 which the user owns peculiarand replies it to a user's client terminal equipment 1. It can limit only to the user who has the memory card 16 in which the MC-Key was memorized by this in the user who can decrypt and use contents JIENKI. Thereforeabove-mentioned contents JIENKI can be safely transmitted only to a regular user.
[0125]Nextthe contents key as which the client terminal equipment 1 was enciphered in Step S16 by MC-Key replied from the system server device 4 side

(Content-Key)Storage control of client ID and HDD-ID which were enciphered by contents JIENKI (Content-Gen-Key) enciphered by MC-Key and contents JIENKI (Content-Gen-Key) is carried out to the memory card 16respectively. Therebythe registration acquisition distance shown in the flow chart of this drawing 7 is completed.

[0126]Thusthis copy management system permits a copy of only the contents memorized by the optical disc which has media unique ID (MID) which did not have a copied history in the past. Therebythe copy of the contents memorized by each optical disc can be restricted at once. For this reasonthe third party to whom the optical disc in which the copy of contents was performed in the past was lent cannot copy contents from that lent optical disc. Thereforemany users can prevent the unauthorized use which copies contents from the optical disc of one sheet.

[0127][Copy of contents] Nexta user is acquiring this contents key (Content-Key)and it becomes possible to copy the contents currently recorded on the optical disc to HDD2.

[0128]The flow chart and drawing 10 which drawing 9 shows the flow of this copy distance are a figure showing typically the information dealt with between the client terminal equipment 1HDD2and the memory card 16when the copy of these contents is performed. The copy distance of contents is explained using this drawing 9 and drawing 10.

[0129]Firstthe flow chart of drawing 9 is started by ending registration of above-mentioned media unique IDand the user who acquired the contents key operating the client terminal equipment 1and specifying the copy of contents.

[0130]In Step S21IOP32 of the client terminal equipment 1 reads the contents key (Content-Key) and contents JIENKI (Content-Gen-Key) which were enciphered by MC-Keyrespectively from the memory card 16These are supplied to CPU30.

[0131]As mentioned aboveMC-Key is heldrespectively with the system server device 4 and this client terminal equipment 1. For this reasonCPU30 carries out decoding processing of the contents key (Content-Key) and contents JIENKI (Content-Gen-Key) which are enciphered [ above-mentioned ] using this MC-Key currently held. And CPU30 carries out storage control of this contents key and contents JIENKI that were decrypted to RAM36. Therebythis copy distance progresses to Step S22.

[0132]In Step S22IOP32 reads client ID and HDD-ID which were enciphered by contents JIENKI (Content-Gen-Key) from the memory card 16and supplies these to CPU30. CPU30 decrypts this client ID and HDD-ID using contents JIENKI (Content-Gen-Key) decrypted previously.

[0133]In this step S22CPU30 compares client ID which decrypted [ above-mentioned ]and client ID given to the client terminal equipment 1 concerned. CPU30 compares HDD-ID which decrypted [ above-mentioned ]and HDD-ID of HDD2 connected to the client terminal equipment 1 concerned.

[0134]Nextin Step S23CPU30 distinguishes whether each above-mentioned client ID and each above-mentioned HDD-ID are in agreementrespectively. When both

are in agreementthis copy distance progresses to Step S24 that the copy of contents should be performed. When both are inharmoniousthis copy distance progresses to Step S28.
[0135]That client ID and HDD-ID which were decrypted from the memory card 16 are not in agreement with client ID of the client terminal equipment 1and HDD-IDIt is shown that acquisition of the above-mentioned contents key (Content-Key) is not performed based on client-terminal-equipment [ of a regular user ] 1 and HDD2.
[0136]That isthe inaccurate user to whom the memory card 16 was lent from the registered user in this case shows that it is trying to copy contents.
[0137]For this reasonCPU30 carries out display control of the message which refuses the copy of the contents of "being unable to copy"for example to a user. By thisthis copy distance will be completed in the interrupted form.
[0138]NextStep S24 is a step which it performs when the client terminal equipment 1 detects coincidence of each above-mentioned client ID and each above-mentioned HDD-ID. In this caseCPU30 decrypts the contents played by the optical-disc-controlling part 33 from the optical disc using the contents key (Content-Key) memorized by RAM36. It re-enciphers by contents JIENKI (Content-Gen-Key) memorized by RAM36and CPU30 supplies these decrypted contents to HDD2.
[0139]Nextin Step S25HDD2 saves the contents re-enciphered by above-mentioned contents JIENKI as shown in drawing 10 at a hard disk (copy).
[0140]Nextat Step S26it is distinguished by CPU30 of the client terminal equipment 1 performing HDD2 and communication whether the copy of contents was completed. When the copy is not completedCPU30 is carrying out repeat execution control of the operation of the above-mentioned step S24 and Step S25and it supplies contents to HDD2 until the copy of contents is completed. Completion of the copy of contents will advance this copy distance to Step S27.
[0141]In Step S27since the copy of contents was completedIOP32 eliminates the contents key (Content-Key) memorized by the memory card 16. Therebythis copy distance is completed.
[0142]Thusthe contents which are enciphered by a contents key (Content-Key) and memorized by the optical disc are decrypted by the contents key published from the system server device 4and the client terminal equipment 1 copies them to HDD2. And the contents key (contents key published from the system server device 4) memorized in the memory card 16 is eliminated after the copy of these contents.
[0143]As mentioned abovein order that a copied history may remain in the database 3 to the optical disc in which the copy of contents was performed in the pastthe recurrence line of a contents key does not perform the system server device 4 in principle. For this reasonthe system server device 4 refuses the copy application from the third party to whom the optical disc in which the copy of contents was performed once was lent based on the copied history of the above-mentioned database. And the system server device 4 does not transmit a contents

key to this third party.
[0144]Since the above-mentioned third party cannot acquire a contents keyhe cannot decrypt the contents memorized by the lent optical disc. For this reasonsince contents cannot be decrypted even if the above-mentioned third party is able to copy contents to secondary-storage mediasuch as HDDthese contents cannot be used. Thereforethis copy management system can prevent the unauthorized use of contents.
[0145][Reproduction of the copied contents] Nexta user can be reincarnated repeatedly and can use now the contents copied to HDD2 in this way.
[0146]The flow chart which shows drawing 11 the flow of the reproduction distance of the contents saved HDD2 is shown. In this reproduction distancethe mimetic diagram of the information dealt with between the client terminal equipment 1HDD2and the memory card 16 is shown in drawing 12.
[0147]The flow chart of drawing 11 is started because the user who terminated the copy of the above-mentioned contents regularly specifies reproduction of contents.
[0148]In Step S31IOP32 of the client terminal equipment 1 reads contents JIENKI (Content-Gen-Key) enciphered by above-mentioned MC-Key from the memory card 16and supplies this to CPU30. CPU30 decrypts this contents JIENKI using MC-Key currently held by the client-terminal-equipment 1 sideand is reproduced.
[0149]Nextin Step S32IOP32 reads client ID and HDD-ID which were enciphered by contents JIENKI (Content-Gen-Key) from the memory card 16and supplies this to CPU30. CPU30 decrypts this client ID and HDD-ID that were enciphered using contents JIENKI decrypted previously.
[0150]Nextin Step S33CPU30 compares client ID given to the client terminal equipment 1 concernedand client ID decrypted by above-mentioned contents JIENKI.
[0151]CPU30 compares HDD-ID of HDD2 connected to the client terminal equipment 1 concernedand HDD-ID decrypted by above-mentioned contents JIENKI.
[0152]That each above-mentioned client ID and each above-mentioned HDD-ID are not in agreement shows that HDD2 of other users' memory card 16other users' client terminal equipment 1or other users is used. For this reasonCPU30 displays the message which refuses reproduction of contents with "unreproducible" contents on a user in Step S35. By thisthe reproduction distance of these contents will be completed in the form interrupted.
[0153]Thusin this copy management systemalso when reproducing the contents copied to HDD2collation of client ID and HDD-ID is performed. For exampleHDD2 where the memory card 16 which a regular user ownsand contents were saved considers the case where it is lent to a third party. A third party will connect HDD2 with this lent memory card 16 to his own client terminal equipmentand the contents memorized in this HDD2 will be reproduced.
[0154]Howeverclient ID memorized in the memory card 16 is a regular user's client ID. For this reasonsince client ID of a third party's client terminal equipment and

client ID memorized by the memory card 16 are not in agreementreproduction of the contents memorized by HDD2 is refused in a third party's client terminal equipment. For this reasoneven when memory card 16 and HDD2 is lentuse of the contents copied to HDD2 can be prevented.
[0155]Nextwhen each above-mentioned client ID and each above-mentioned HDD2 are in agreementrespectivelyCPU30 decrypts the contents of HDD2 using contents JIENKI decrypted previouslyand memorizes this to RAM36. Therebythe reproduction distance of these contents is completed.
[0156]When the contents memorized by RAM36 are game contents of a video gamefor exampleCPU30 operates based on these game contents. And CPU30 carries out display control of the character of a video gamefor exampleand carries out pronunciation control of a sound effectBGMetc. Therebythe user can enjoy a video game based on the game contents copied to HDD2 from an optical disc.
[0157]When playing game contents directly from an optical disc and performing a video gamewhenever it performs a new video gamethe detaching work of an optical disc is required. Howeverthe detaching work of the optical disc which was needed whenever it performed a new video game is omissible by copying to HDD2 the game contents recorded on each optical disc in this way. For this reasonthe start of a new video game can be enabled smoothly.
[0158]Since the contents key memorized by the memory card 16 is eliminated after the copy of contents is completed from an optical discthe re-copy of contents cannot be performed. Howevercontents JIENKI memorized by the memory card 16 is not eliminated even after the completion of a copy. For this reasonthe contents which were enciphered by contents JIENKI and copied to HDD2 are repeatedly decrypted using contents JIENKI memorized by this memory card 16and are refreshable.
[0159][Correspondence over repair of a device and exchange] Nextin the case of this copy management systemclient IDHDD-IDMC-ID (collectively henceforth a device ID)etc. and user ID are put in block as user entry informationand the system server device 4 manages them. Howeverwhen the client terminal equipment 1 and the device of HDD2 grade are exchanged by breakage etc.the device ID of this exchanged device differs from the device ID registered as user entry information. Thereforewhen devices are exchangedin spite of being a regular userwe are anxious about the copy and reproduction of contents becoming impossible using the exchanged device.
[0160]On the other handin the case of this copy management systemthe unauthorized use of contents is prevented by securing the indigenity of a device ID. For this reasoneven when repair restores the client terminal equipment 1 and the device of HDD2 gradethe device after this repair is receivedIt is preferred to attach a different new device ID from the device ID attached before repairto distinguish the device before repair and the device after repair clearlyand to manage them.
[0161]Howeverlike the time of exchange of the above-mentioned deviceif a new device ID is attached to the device after repair in this wayin spite of being a

regular userwe will be anxious about the copy and reproduction of contents becoming impossible using the fixed device.
[0162]This copy management system has prevented as follows the above-mentioned inconvenience about which we are anxious by using a new device ID by repair and exchange of a device.
[0163][Correspondence over repair of client terminal equipment and HDDand exchange] The mimetic diagram for explaining the correspondence over repair of the client terminal equipment in this copy management system and HDD and exchange is shown in drawing 13. Client-terminal-equipment 1 or HDD2 on which x seal is drawn shows the damaged device among this drawing 13.
[0164]In this drawing 13when a device is damageda user sends that damaged device to the repair center by the side of the administrator who manages this copy management system with the memory card 16.
[0165]Namelyalthough the memory card 16 is not damaged in this caseClient ID and HDD-ID (each ID is hereafter called device ID collectively) which were enciphered by contents JIENKI (Content-Gen-Key) or contents JIENKI (Content-Gen-Key) are memorized by the memory card 16. For this reasoneven when a device is damagedthe memory card 16 is sent to the above-mentioned repair center with this damaged device (or carrying in).
[0166]In a repair centerif the broken device is sentit will fix and exchange so that this device may operate normallyand a new device ID is given to devices carried outsuch as this repair and exchange.
[0167]Specificallyclient ID of the client terminal equipment 1 is memorized by MASK-ROM35for example with above-mentioned hardware ID and an operating system program. The same MASK-ROM as the above-mentioned MASK-ROM35 is provided also in HDD2and HDD-ID is memorized by this MASK-ROM. For this reasonin a repair centerwhen a device is fixed. MASK-ROM provided before performing this repair is removedand grant of new client ID or HDD-ID is performed by exchanging for MASK-ROM new client ID or HDD-ID was remembered to be.
[0168]Since a different device ID from the device broken in MASK-ROM of this new device is memorized when exchanging the device itself for a new deviceexchange of MASK-ROM like [ at the time of the above-mentioned repair ] is not performed.
[0169]Nextthe operator of a repair center reproduces MC-ID of the memory card 16 sent with the broken device. An operator accesses the database 3 of the above-mentioned system server device 4 via the terminal unit formed in the repair centerand refer to the user entry information memorized by the above-mentioned database 3 for it based on MC-ID reproduced from the above-mentioned memory card 16. And an operator operates a terminal unit and carries out correction registration of the device ID among the user entry information memorized by this database 3 at the newly given device ID. An operator operates the database 3 via a terminal unitand takes down the above-mentioned flag set to copied contents.
[0170]Contents JIENKI (Content-Gen-Key) which an operator operates a terminal

unit and is memorized in the memory card 16 and which was enciphered by MC-KeyThe device ID (client ID and HDD-ID) enciphered by contents JIENKI (Content-Gen-Key) is eliminatedrespectively. And this memory card 16 is returned to a user with the exchanged device [ fix and ] (or personal delivery).
[0171]By thisthe state of a user's device (the client terminal equipment 1HDD2and memory card 16) will return to the state (state just before copying = contents) immediately after completing the user registration distance explained using drawing 5 and drawing 6.
[0172]The user to whom this memory card 16 and device were returned operates the client terminal equipment 1 so that registration of media unique ID (MID) explained using drawing 7 and drawing 8 and acquisition of a contents key (Content-Key) may be performed again.
[0173]The client terminal equipment 1 accesses the system server device 4 corresponding to a user's operationand registers media unique ID (MID). And the client terminal equipment 1 re-copies to HDD2 the contents memorized by the optical disc using the contents key (Content-Key) acquired from the system server device 4 by this registration.
[0174]Therebyif it is a regular user even when repair and exchange of a device newly give a device IDexecution of the copy and reproduction of contents can be enabled based on a new device ID.
[0175]In the copy management system sideby attaching a new device ID to the device restored by repair or exchangethe device before repair and the device after repair can be distinguished clearlyand can be managed.
[0176][Correspondence over breakage of a memory cardand loss] Nextin the case of this copy management systemto breakage of the memory card 16or lossit is coped with as follows. The mimetic diagram for explaining the correspondence over breakage of the memory card 16 in this copy management system and loss is shown in drawing 14. The memory card 16 surrounded and shown by the frame of a dotted line shows the memory card 16 damaged or lost among this drawing 14.
[0177]When the memory card 16 is damaged or lostas shown in this drawing 14a user connects the client terminal equipment 1 to the system server device 4 via the Internet 5and applies for the recurrence line of a memory card to the system server device 4.
[0178]If this application is madethe system server device 4 will transmit the input screen data of user ID to the client-terminal-equipment 1 side. Therebya user's client terminal equipment 1 carries out display control of the input screen of user ID to the television receiver 18.
[0179]A user inputs user ID to this input screen. Howeversince the memory card 16 is damaged or lost in this caseuser ID (User ID) cannot be read from the memory card 16. For this reasona user inputs user IDseeing the user ID copied into the memo pad etc.when user ID is published. The client terminal equipment 1 transmits this inputted user ID to the system server device 4.
[0180]Nextrefer to the user entry information corresponding to the user ID transmitted by this user for the system server device 4 from the database 3.

Therebythe system server device 4 can recognize the contents etc. which were copied with contents JIENKI (Content-Gen-Key) or its memory card 16 with MC-ID and MC-Key of the memory card 16 which were damaged or lost.
[0181]Nextthe system server device 4 receives memory card 16new which has new MC-IDNew MC-Key (New-MC-Key) and contents JIENKI (Content-Gen-Key) newly enciphered by this New-MC-KeyClient ID and HDD-ID which were enciphered by this contents JIENKI (Content-Gen-Key) are rerecorded. The system server device 4 rewrites MC-IDMC-Keyetc. so that the user entry information memorized by the database 3 may turn into user entry information corresponding to this new memory card 16New.
[0182]It is a case where the memory card 16 is damaged or lost in this caseand client-terminal-equipment [ of a user ] 1 and HDD2 is operating normally. For this reasonas client ID enciphered by contents JIENKI (Content-Gen-Key)and HDD-IDthe original device ID is used as it is.
[0183]Nexta repair center sends this memory card 16new to the user side physicallyfor example by mail etc. As mentioned abovein the system server device 4 sidethe user entry information of the database 3 is rewritten with rewriting of each information in this memory card 16new. For this reasonthe user who received sent memory card 16new can perform copy of contentscopied reproduction of contentsetc. like before using this memory card 16newthe client terminal equipment 1and the system of the combination of HDD2.
[0184][Effect of a 1st embodiment] The copy management system of this 1st embodiment stores the contents to which the system administrator performed encryption processing by the contents key in the optical disc in which media unique ID (MID) was givenand is distributed to a user so that clearly from the above explanation.
[0185]When a user copies contentshe transmits MID of an optical disc to the system server device 4. A user transmits the device IDs (client IDHDD-IDMC-IDetc.) of the device which he is using to the system server device 4.
[0186]The system server device 4 was related with the device ID of the device which each user is usingand MID of the optical disc in which the copy of contents was performed in the past is memorized in the database 3.
[0187]MID of the device ID and optical disc in which the user is using the system server device 4 when the copy application of contents is made from a user -- it is based and the database 3 is referred to. The system server device 4 transmits the contents key for decrypting contentson condition that the MID same in the database 3 is not registered to a user's client terminal equipment 1.
[0188]The client terminal equipment 1 decrypts the contents memorized by the optical disc using this contents keyand copies them to HDD2.
[0189]When this copy management system puts up the same MID as MID registered into the database 3 and a copy application is madedistribution of the above-mentioned contents key is not performed. For this reasonthis copy management system can restrict the copy of contents at onceand can prevent the illegal copy of contents.

[0190][A 2nd embodiment] The copy management system which serves as a 2nd embodiment of this invention next is explained. The copy management system of a 1st above-mentioned embodiment registers as a user by a user connecting his own client terminal equipment 1 to the system server device 4 by the side of a system administrator directlyacquires a contents key (Content-Key) etc.and copies contents.
[0191]The 3rd person management server device with which the 3rd person manages the copy management system of this 2nd embodiment between a user's client terminal equipment 1 and the system server device 4 by the side of a system administrator is formed. A user acquires a contents key (Content-Key) etc. via this 3rd person management server device. The 3rd person management server device performs fee collection to offer of this contents key (Content-Key).
[0192][Composition of a 2nd embodiment] The system configuration figure of the copy management system used as this 2nd embodiment is shown in drawing 15. When this drawing 15 copies contents from an optical discit shows the flow which acquires a contents key (Content-Key).
[0193]As for the system server device 4 and the 3rd person management server device 50in this drawing 15the dedicated line and the public line are mutually connected by available VPN (VirtualPrivate Network) etc. like a dedicated linefor example.
[0194]The system server device 4 is not connected to the Internet 5but this 3rd person management server device 50 is connected to the Internet 5. For this reasonthe user cannot access directly to the system server device 4but will access the system server device 4 indirectly via this 3rd person management server device 50.
[0195][Operation of a 2nd embodiment] Nextexplanation of the copy management system of this 2nd embodiment of operation is given. In the case of the copy management system of this 2nd embodimentthe user who tries to copy contents connects his own client terminal equipment 1 to the 3rd person management server device 50 via the Internet 5 from an optical disc. And a user transmits MC-IDuser ID (User ID)and media unique ID (MID) to the 3rd person management server device 50 side via the client terminal equipment 1. A user transmits the account information for 3rd person management server device 50 (for examplea user namea passwordetc.) to the 3rd person management server device 50 via the client terminal equipment 1.
[0196]The client terminal equipment 1 transmits MC-ID and account information to the 3rd person management server device 50 as it is. The client terminal equipment 1 enciphers user ID (User ID) and media unique ID (MID) of an optical disc by MC-Keyand transmits these to the 3rd person management server device 50.
[0197]The 3rd person management server device 50 extracts and acquires account information among each information transmitted from the client terminal equipment 1. The 3rd person management server device 50 transmits the user ID (User ID) enciphered by MC-ID and MC-Key via the dedicated line (or the above-

mentioned VPN)and media unique ID (MID) enciphered by MC-Key to the system server device 4.
[0198]If this MC-IDuser IDand MID are receivedthe system server device 4The contents key (Content-Key) for decrypting the contents which are similarly enciphered as the above-mentioned and are recorded on the optical disc is enciphered by MC-Keyand it replies to the 3rd person management server device 50. The system server device 4 enciphers contents JIENKI (Content-Gen-Key) by MC-Keyand replies it to the 3rd person management server device 50. Furthermorethe system server device 4 enciphers a user's client ID and HDD-ID by this contents JIENKI (Content-Gen-Key)and replies them to the 3rd person management server device 50.
[0199]The contents key as which the 3rd person management server device 50 was enciphered by this MC-Key (Content-Key)Contents JIENKI enciphered by MC-Key (Content-Gen-Key)And a user's client ID enciphered by contents JIENKI (Content-Gen-Key) and HDD-ID are transmitted to a user's client terminal equipment 1 via the Internet 5respectively.
[0200]The 3rd person management server device 50 performs fee collection to the user based on the account information for 3rd person management server device 50 previously transmitted from the client terminal equipment 1 in compensation for having provided the contents key (Content-Key).
[0201]The client terminal equipment 1 carries out storage control of the above-mentioned contents key transmitted from the 3rd person management server device 50contents JIENKIclient IDand HDD-ID to the memory card 16and uses them for reproduction of the contents which contents copied and copied as mentioned above.
[0202]The number of a user's credit card and the amount information by which prepaid one was carried out are beforehand registered into the 3rd person management server device 50 sidefor example. For this reasona credit card company is asked for the amount of money charged in exchange for offer of a contents keyand the 3rd person management server device 50 collects it. Or the 3rd person management server device 50 subtracts and collects the charged amount of money from the balance by which prepaid one is carried out.
[0203]For example between the administrator of the system server device 4and the administrator of the 3rd person management server device 50the money collected in this way will be distributed at a predetermined rate.
[0204][Effect of a 2nd embodiment] The copy management system of this 2nd embodiment forms and constitutes the 3rd person management server device 50 between the client terminal equipment 1 and the system server device 4 in this way. A user accesses the system server device 4 via this 3rd person management server device 50and charges distribution of a contents key (Content-Key). The 3rd person management server device 50 is charged by distributing this contents key (Content-Key) to a user.
[0205]Therebythis copy management system can provide a new copy management system called the copy management system with which the 3rd person

(administrator of the 3rd person management server device 50) intervenesand also can acquire the same effect as the copy management system of a 1st above-mentioned embodiment.

[0206]Contents can be distributed gratuitously to a user via a predetermined network via an optical disc etc. by charging itwhen this copy management system distributes a contents key to a user.

[0207]In this copy management systemwhen a user is supplied widely and there is an application of a copy from a userwithout giving MID to an optical discthe system server device 4 or the 3rd person management server device 50 may be made to charge by distributing a contents key to that user.

[0208]Although it presupposed that the 3rd person management server device 50 charges the copy management system of this 2nd embodimentthe system server device 4 may be made to charge this.

[0209]Finallythis invention is not limited to each above-mentioned embodiment described as an example. For this reasonif it is a range which does not deviate from the technical idea concerning this invention even if it is except each above-mentioned embodimentof course according to a design etc.various change is possible.

[0210]For examplein explanation of each above-mentioned embodimentit was presupposed to the client terminal equipment 1 as device identification information that client IDHDD-IDand MC-ID are transmitted to the system server device 4. Howeveronly client ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarlyonly HDD-ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarlyonly MC-ID may be transmitted to the system server device 4 from the client terminal equipment 1.

[0211]Client ID and HDD-ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarlyclient ID and MC-ID may be transmitted to the system server device 4 from the client terminal equipment 1. SimilarlyHDD-ID and MC-ID may be transmitted to the system server device 4 from the client terminal equipment 1.

[0212]That isthe copy management system of each above-mentioned embodiment prevents an illegal copy by associating the storage with which the copy of contents is performedand the device used for the copy of contentsand performing copy management by the system server device 4 side. For this reasonas device identification information transmitted to the system server device 4 from the client terminal equipment 1what is necessary is just the identification information which can specify a user.

[0213]Although we decided to use the memory card 16 in explanation of each above-mentioned embodimentwhen it is this copy management systemthe memory card 16 is not necessarily needed. What is necessary is just to make the memory built in HDD2 or the client terminal equipment 1 memorize the above-mentioned contents key memorized by the memory card 16contents JIENKIetc.when not using the memory card 16.

[0214]
[Effect of the Invention]This invention can permit the copy of the contents memorized by the storage only to the regular user who is an owner of a storage. For this reasonthe illegal copy of the contents memorized by the storage can be prevented.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the system configuration of the copy management system of a 1st embodiment of this invention.
[Drawing 2]It is a perspective view showing the appearance of the client terminal equipment which constitutes a copy management systemand a hard disk drive (HDD).
[Drawing 3]It is a block diagram showing the electric composition of client terminal equipment.
[Drawing 4]It is the figure for explaining the optical disc used for this copy management system with which the digital contents enciphered by the contents key (Content-Key) were memorized.
[Drawing 5]It is a flow chart which shows the flow of the user registration in a copy management system.
[Drawing 6]It is a mimetic diagram of the copy management system in which each information transmitted and received between client terminal equipment and a system server device at the time of user registration is shown.
[Drawing 7]It is a flow chart which shows the register operation of media unique ID (MID) in a copy management system individually given to the optical discand the acquisition operation of a contents key (Content-Key).
[Drawing 8]It is a mimetic diagram of the copy management system in which each information transmitted and received between client terminal equipment and a system server device at the time of registration of media unique ID (MID) individually given to the optical disc and acquisition of a contents key (Content-Key) is shown.
[Drawing 9]It is a flow chart which shows the flow of the copy distance in a copy management system.
[Drawing 10]It is a mimetic diagram showing each information transmitted and received between client terminal equipmenta memory cardand a hard disk drive at the time of copy execution.
[Drawing 11]It is a flow chart which shows the reproduction motion of the digital contents copied to the hard disk drive in a copy management system.
[Drawing 12]It is a mimetic diagram showing the information transmitted and received between client terminal equipmenta memory cardand a hard disk drive at the time of reproduction of the digital contents copied to the hard disk drive.
[Drawing 13]It is a mimetic diagram for explaining correspondence of the copy

management system to repair or exchange of client terminal equipment or a hard disk drive.

[Drawing 14]It is a mimetic diagram for explaining correspondence of the copy management system to breakage or loss of a memory card.

[Drawing 15]At the time of registration of media unique ID (MID) individually given to the optical disc. And it is a mimetic diagram of the copy management system used as a 2nd embodiment of this invention showing each information transmitted and received between client terminal equipment and a system server device at the time of acquisition of a contents key (Content-Key).

[Description of Notations]

1 [ -- A system server device 5 / -- The Internet6 / -- Communication MODEM ] -- Client terminal equipment2 -- A hard disk drive (HDD)3 -- A database4

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－328846
（P2002－328846A）
(43)公開日　平成14年11月15日(2002.11.15)

| (51)Int.Cl.⁷ | | 識別記号 | FI | | テーマコード（参考） |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３２０ | Ｇ０６Ｆ 12/14 | ３２０Ｅ | ５Ｂ０１７ |
| | | | | ３２０Ｆ | ５Ｊ１０４ |
| | 17/60 | １４２ | 17/60 | １４２ | |
| | | ３０２ | | ３０２Ｅ | |
| | | ３３２ | | ３３２ | |

審査請求　有　　請求項の数18　ＯＬ　（全 28 頁）　最終頁に続く

(21)出願番号　特願2002－41890(P2002－41890)

(22)出願日　平成14年２月19日(2002.2.19)

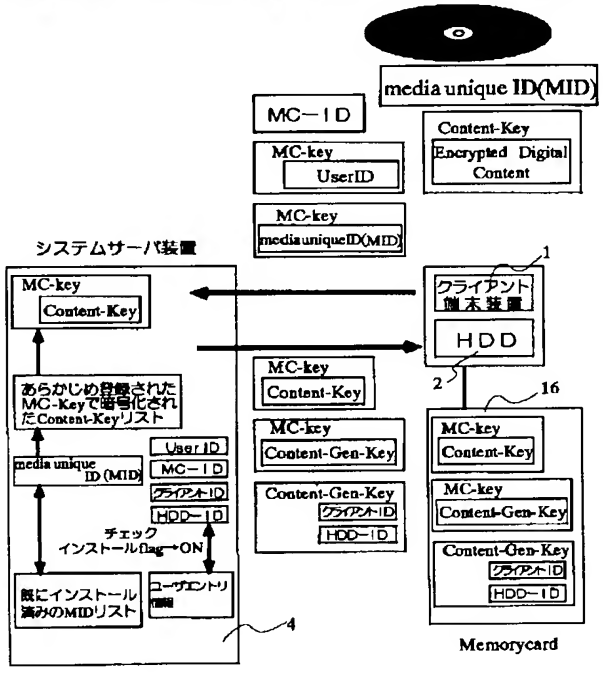
(31)優先権主張番号　特願2001－44358(P2001－44358)
(32)優先日　平成13年２月20日(2001.2.20)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　395015319
株式会社ソニー・コンピュータエンタテインメント
東京都港区赤坂７－１－１
(72)発明者　島田　宗毅
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(74)代理人　100107238
弁理士　米山　尚志

最終頁に続く

(54)【発明の名称】　コピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取

(57)【要約】
【課題】　コンテンツの不正コピーを防止する。
【解決手段】　各光ディスク毎にＩＤ（MID）を付すと共に、コンテンツをContent-Keyで暗号化して記録しておく。システムサーバ装置は、ユーザが所有するクライアント端末装置のクライアントＩＤ，ＨＤＤのHDD-ID、及びメモリカードのMC-ID等をユーザエントリ情報として管理する。ユーザはコンテンツのコピーを行う際に、光ディスクのMIDと共にMC-IDをシステムサーバ装置に送信する。システムサーバ装置は、MC-IDをユーザエントリ情報と照合してユーザを特定し、コンテンツの暗号化の際に用いたContent-Keyを返送する。ユーザ側では、この返送されたContent-Keyを用いて光ディスクに記録されているコンテンツを復号化しＨＤＤにコピーする。記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーが許可されるため、コンテンツの不正コピーを防止することができる。



【特許請求の範囲】
【請求項１】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付され、管理者側からユーザに配布される記憶媒体と、
上記記憶媒体に記憶されているコンテンツを、上記暗号化鍵に対応する復号化鍵を用いて復号化して二次記憶媒体にコピーするコピー機能を有し、該コンテンツのコピーを行う際に、上記記憶媒体の媒体識別情報と共に、所定かつ固有のデバイス識別情報を送信するユーザの端末装置と、
上記記憶媒体の媒体識別番号を受信した際に、上記デバイス識別情報を有するユーザの端末装置に対して、上記コンテンツの復号化鍵を送信する管理サーバ装置とを有するコピー管理システム。
【請求項２】　請求項１記載のコピー管理システムであって、
上記管理サーバ装置は、一つの媒体識別情報に対して１回のみ復号化鍵の送信を行うことを特徴とするコピー管理システム。
【請求項３】　請求項１又は請求項２記載のコピー管理システムであって、
上記端末装置は、上記端末装置の識別情報、上記コンテンツのコピーを行うコピー手段に固有に付された識別情報、及び外付けの半導体メモリに固有に付された識別番号のうち、いずれか１つ或いは複数を組み合わせ、上記デバイス識別情報として送信することを特徴とするコピー管理システム。
【請求項４】　請求項１から請求項３のうち、いずれか一項記載のコピー管理システムであって、
上記管理サーバ装置は、上記デバイス識別情報で上記復号化鍵を暗号化して送信し、
上記端末装置は、自己のデバイス識別情報で、上記暗号化された復号化鍵を復号化して用いることを特徴とするコピー管理システム。
【請求項５】　請求項１から請求項４のうち、いずれか一項記載のコピー管理システムであって、
上記端末装置は、上記コンテンツの復号化後に、上記復号化鍵を削除することを特徴とするコピー管理システム。
【請求項６】　請求項１から請求項５のうち、いずれか一項記載のコピー管理システムであって、
上記管理サーバ装置は、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信し、
上記端末装置は、上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーし、上記再暗号化鍵を記憶手段に記憶し、上記記憶手段に記憶した再暗号化鍵を用いて、上記コピーされたコンテンツを復号化して再生することを特徴とするコピー管理システム。
【請求項７】　請求項１から請求項６のうち、いずれか一項記載のコピー管理システムであって、
上記管理サーバ装置は、各ユーザのデバイス識別情報に関連付けして上記復号化鍵を送信済みの媒体識別情報をデータベースに記憶することで上記復号化鍵の配信管理を行い、修理或いは交換によりユーザのデバイス識別情報が変更された場合、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えることを特徴とするコピー管理システム。
【請求項８】　請求項１から請求項７のうち、いずれか一項記載のコピー管理システムであって、
上記管理サーバ装置は、復号化鍵の送信を行った端末装置を有するユーザに対して所定の課金処理を行うことを特徴とするコピー管理システム。
【請求項９】　請求項１から請求項８のうち、いずれか一項記載のコピー管理システムであって、
上記ユーザの端末装置と上記管理サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記復号化鍵をユーザの端末装置に送信した際に、ユーザに対する課金処理を行う仲介サーバ装置を有することを特徴とするコピー管理システム。
【請求項１０】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、
ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、
少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、
上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、
上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、
上記復号化処理したコンテンツをコピーするステップとを有するクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項１１】　請求項１０記載の記憶媒体であって、
上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、
上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理することを特徴とする記憶媒体。
【請求項１２】　請求項１０又は請求項１１記載の記憶媒体であって、
上記コンテンツのコピー後に、上記復号化鍵を削除するステップを有することを特徴とする記憶媒体。
【請求項１３】　請求項１０から請求項１２のうち、い

ずれか一項記載の記憶媒体であって、
上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、
上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、
上記再暗号化鍵を記憶手段に記憶するステップと、
コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップとを有することを特徴とする記憶媒体。
【請求項１４】　請求項１０から請求項１３のうち、いずれか一項記載の記憶媒体であって、
上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信することを特徴とする記憶媒体。
【請求項１５】　ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、
各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップとを有する管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項１６】　請求項１５記載の記憶媒体であって、
上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有することを特徴とする記憶媒体。
【請求項１７】　請求項１５又は請求項１６記載の記憶媒体であって、
上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信することを特徴とする記憶媒体。
【請求項１８】　請求項１５から請求項１７のうち、いずれか一項記載の記憶媒体であって、
上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信することを特徴とする記憶媒体。
【請求項１９】　請求項１５から請求項１８のうち、いずれか一項記載の記憶媒体であって、
修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有することを特徴とする記憶媒体。
【請求項２０】　請求項１５から請求項１９のうち、いずれか一項記載の記憶媒体であって、
上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有することを特徴とする記憶媒体。
【請求項２１】　請求項１５から請求項２０のうち、いずれか一項記載の記載の記憶媒体であって、
上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする記憶媒体。
【請求項２２】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、
ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、
少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、
上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、
上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、
上記復号化処理したコンテンツをコピーするステップとを有するクライアント端末装置の情報処理プログラム。
【請求項２３】　請求項２２記載の情報処理プログラムであって、
上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、
上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理することを特徴とする情報処理プログラム。
【請求項２４】　請求項２２又は請求項２３記載の情報処理プログラムであって、
上記コンテンツのコピー後に、上記復号化鍵を削除する

ステップを有することを特徴とする情報処理プログラム。

【請求項２５】　請求項２２から請求項２４のうち、いずれか一項記載の情報処理プログラムであって、
上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、
上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、
上記再暗号化鍵を記憶手段に記憶するステップと、
コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップとを有することを特徴とする情報処理プログラム。

【請求項２６】　請求項２２から請求項２５のうち、いずれか一項記載の情報処理プログラムであって、
上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信することを特徴とする情報処理プログラム。

【請求項２７】　ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、
各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、
上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップとを有する管理サーバ装置の情報処理プログラム。

【請求項２８】　請求項２７記載の情報処理プログラムであって、
上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有することを特徴とする情報処理プログラム。

【請求項２９】　請求項２７又は請求項２８記載の情報処理プログラムであって、
上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信することを特徴とする情報処理プログラム。

【請求項３０】　請求項２７から請求項２９のうち、いずれか一項記載の情報処理プログラムであって、
上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信することを特徴とする情報処理プログラム。

【請求項３１】　請求項２７から請求項３０のうち、いずれか一項記載の情報処理プログラムであって、
修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有することを特徴とする情報処理プログラム。

【請求項３２】　請求項２７から請求項３１のうち、いずれか一項記載の情報処理プログラムであって、
上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有することを特徴とする情報処理プログラム。

【請求項３３】　請求項２７から請求項３２のうち、いずれか一項記載の記載の情報処理プログラムであって、
上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする情報処理プログラム。

【請求項３４】　固有のデバイス識別番号が付されたユーザのデバイスで、固有の媒体識別情報が付された記憶媒体に暗号化鍵で暗号化されて記憶されているコンテンツのコピーを行う際に、上記デバイスから上記デバイス識別情報及び上記媒体識別情報を管理サーバ装置に送信し、
コンテンツのコピーが行われた記憶媒体の媒体識別情報が、各ユーザのデバイスのデバイス識別情報に関連付けされた状態で登録されるデータベースに、上記ユーザのデバイスから送信された媒体識別情報が登録されているか否かを上記管理サーバ装置が検出し、
上記データベースに、上記媒体識別情報が未登録であった場合に、上記管理サーバ装置からユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するコピー管理方法。

【請求項３５】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出し、
ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出し、
少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信し、
上記媒体識別情報及びデバイス識別情報を送信すること

で、上記管理者側のサーバ装置から返信される復号化鍵を受信し、
上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理し、
上記復号化処理したコンテンツをコピーするクライアント端末装置の情報処理方法。
【請求項３６】　ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信し、
各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出し、
上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する管理サーバ装置の情報処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばゲームコンテンツ，映画コンテンツ，音楽コンテンツ，アプリケーションプログラム等のコンピュータプログラムのコピー管理を行うコピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法に関する。
【０００２】
【従来の技術】今日において、例えばＣＤ－ＲＯＭ，ＤＶＤ－ＲＯＭ或いは半導体メモリ等の記憶媒体に記憶されているゲームコンテンツに基づいてビデオゲームを実行するビデオゲーム機が広く普及している。
【０００３】ユーザは、所望のゲームコンテンツが記憶された記憶媒体を購入し、この記憶媒体をビデオゲーム機で再生してビデオゲームを行う。大抵の場合、ユーザは、徐々に新しいビデオゲームを買い揃えていく。このため、月日と共にユーザの手元には各ゲームコンテンツが記憶された記憶媒体が蓄積されていくこととなる。
【０００４】しかし、ビデオゲーム機には、記憶媒体の再生機構が１基のみ設けられている場合が多い。このため、異なるビデオゲームを行う場合には、ビデオゲーム機に現在装着されている記憶媒体を取り出し、これから行おうとするゲームコンテンツが記憶された記憶媒体を新たに装着し直すという、大変面倒な作業を必要としていた。
【０００５】
【発明が解決しようとする課題】本件出願人は、例えば数十Ｇ（ギガ）オーダーの大容量のハードディスクドライブ（ＨＤＤ）を内蔵或いは外付け可能としたビデオゲーム機を開示している。
【０００６】このビデオゲーム機の場合、各記憶媒体に記憶されているゲームコンテンツをそれぞれＨＤＤにコピーし、このＨＤＤから所望のゲームコンテンツを再生して利用することができる。このＨＤＤを用いることにより、ビデオゲーム機の再生機構に記憶媒体を着脱する手間を省略することができる。
【０００７】ここで、ゲームコンテンツ等のコンピュータプログラムは、そのコンピュータプログラムが記憶されたソフトウェアを購入する等して正当に入手したユーザのみが使用可能なはずである。
【０００８】しかし、記憶媒体に記憶されたコンピュータプログラムを二次記憶媒体にコピー可能とした場合、一つの記憶媒体に記憶されているコンピュータプログラムを、複数のユーザがそれぞれ二次記憶媒体にコピーして使用する不正コピーが懸念される。
【０００９】本発明は、上述の課題に鑑みてなされたものであり、正当なユーザに対してのみ、コンピュータプログラムのコピーを可能とするコピー管理を行うことで、コンテンツの不正使用の防止等を図ったコピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法の提供を目的とする。
【００１０】
【課題を解決するための手段】本発明は、暗号化鍵で暗号化したコンテンツを記憶させた記憶媒体に対して固有の識別番号を付してユーザに配布する。ユーザがコンテンツのコピーを行う際に使用するデバイスにも識別番号が付されている。
【００１１】上記デバイスは、コンテンツのコピーを行う際に、上記記憶媒体の識別番号、及びデバイスの識別番号を管理サーバ装置に送信する。管理サーバ装置は、各ユーザが使用するデバイスの識別番号が登録されたデータベースを有している。管理サーバ装置は、データベースに登録されているデバイスの識別番号と、ユーザのデバイスから送信されたデバイスの識別番号とを照合してユーザを特定する。管理サーバ装置は、この照合を行うことでユーザが特定された際に、記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザのデバイスに送信する。
【００１２】ユーザのデバイスは、この管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されて

いるコンテンツを復号化してコンテンツのコピーを行う。

【００１３】これにより、記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーを許可することができ、コンテンツの不正コピーを防止することができる。

【００１４】

【発明の実施の形態】本発明は、コンピュータプログラムのコピー管理を行うコピー管理システムに適用することができる。

【００１５】コンピュータプログラムとしては、例えばゲームコンテンツ，音楽コンテンツ，映画コンテンツ，アプリケーションプログラム等がある。また、コンピュータプログラムが記憶された記憶媒体としては、ＤＶＤ－ＲＯＭ，ＣＤ－ＲＯＭ等の光ディスクの他、半導体メモリがある。また、コンピュータプログラムのコピー先となる二次記憶媒体としては、ハードディスク（ＨＤ），ＤＶＤ－ＲＡＭや光磁気ディスク（ＭＯ）等がある。

【００１６】以下、上記ゲームコンテンツ，音楽コンテンツ，映画コンテンツ，アプリケーションプログラム等を総称して、単に「コンテンツ」ということとする。

【００１７】［コピー管理システムの全体構成］まず、図１に本発明の第１の実施の形態となるコピー管理システムの全体構成を示す。この図１に示すように、この第１の実施の形態のコピー管理システムは、光ディスクに記憶されているコンテンツの再生機能（実行機能）、及びネットワークを介した通信機能を備えたクライアント端末装置１を有している。

【００１８】このクライアント端末装置１には、光ディスクに記憶されたコンテンツをコピーするためのハードディスクドライブ２（ＨＤＤ）が接続されている。

【００１９】また、このクライアント端末装置１には、インターネット５などのネットワークとの接続を図るための通信モデム６が接続されている。

【００２０】なお、通信モデム６は、この図１に示すようにクライアント端末装置１に対して外付けのかたちで設けてもよい。また、通信モデム６は、クライアント端末装置１に内蔵のかたちで設けてもよい。

【００２１】また、コピー管理システムは、ユーザエントリ情報が記憶されたデータベース３を備えたシステムサーバ装置４を有している。

【００２２】このシステムサーバ装置４と上記クライアント端末装置１とが、例えばインターネット５等のネットワークを介して相互に接続されることでこの第１の実施の形態のコピー管理システムが構成されている。

【００２３】［クライアント端末装置の構成］図２に、クライアント端末装置１の外観の斜視図を示す。この図２示すように、クライアント端末装置１の前面側には、コントローラ接続部７Ａ，７Ｂと、メモリカード装着部８Ａ，８Ｂが設けられている。

【００２４】また、このクライアント端末装置１の前面側には、ＵＳＢ対応機器（ＵＳＢ：Universal Serial Bus）が接続される２つのＵＳＢ接続端子９と、例えば最大４００Ｍｂｐｓのデータ転送速度に対応可能なＩＥＥＥ１３９４接続端子１０とが設けられている。

【００２５】また、このクライアント端末装置１の前面側には、光ディスクが装着されるトレイ型のディスク装着部１１が設けられている。

【００２６】また、このクライアント端末装置１の前面側には、コンテンツの実行動作や再生動作をリセットするためのリセットボタン１２と、光ディスク装着部１１のトレイの出し入れを操作するためのトレイ操作ボタン１３とが設けられている。

【００２７】クライアント端末装置１の背面側には、電源スイッチ、音声映像出力端子（ＡＶマルチ出力端子）、ＰＣカードスロット、光デジタル出力端子、ＡＣ電源入力端子等が設けられている。

【００２８】ＡＶマルチ出力端子は、ＡＶケーブル１７を介してモニタ用のテレビジョン受像機１８に接続される。クライアント端末装置１から出力される映像信号や音声信号は、このＡＶマルチ出力端子及びＡＶケーブル１７を介してモニタ用のテレビジョン受像機１８に供給される。これにより、上記コンテンツの映像がテレビジョン受像機１８に表示される。また、上記コンテンツの音声がテレビジョン受像機のスピーカ装置を介して発音される。

【００２９】コントローラ接続部７Ａ、７Ｂには、コントローラケーブル１５を介してそれぞれコントローラ１４が接続される。

【００３０】メモリカード装着部８Ａ、８Ｂには、ゲームデータのセーブ（記憶）及び読み出しを行うセーブ用のメモリカード等が装着される。

【００３１】［ハードディスクドライブの構成］次に、図２において、クライアント端末装置１の上面部に載置されている筐体がハードディスクドライブ２（以下、ＨＤＤ２という）である。このＨＤＤ２は、内部に例えば４０ＧＢ等の大容量のハードディスクが設けられている。このＨＤＤ２には、十数枚分のＤＶＤ－ＲＯＭに記憶されたゲームコンテンツをコピー可能となっている。

【００３２】ＨＤＤ２の前面側には、電源投入時に点灯駆動される電源ランプ２０と、ハードディスクへの書き込みに連動して点灯駆動される書き込み表示ランプ２１とが設けられている。ＨＤＤ２の背面側には、少なくとも電源スイッチ及びデータ入出力端子が設けられている。

【００３３】ＨＤＤ２をクライアント端末装置１に接続する場合、クライアント端末装置１の背面側に設けられた上記ＰＣカードスロットにＰＣカードを挿入する。この状態で、ＰＣカードに接続ケーブルの一端を接続す

る。接続ケーブルの他端は、ＨＤＤ２のデータ入出力端子に接続する。これにより、クライアント端末装置１とＨＤＤ２とが、電気的に相互に接続される。

【００３４】なお、この例においては、ＨＤＤ２はクライアント端末装置１とは別体で、クライアント端末装置１に対して外付けすることとした。しかし、このＨＤＤ２を、クライアント端末装置１に内蔵するかたちで設けてもよい。

【００３５】また、クライアント端末装置１とＨＤＤ２とをＰＣカードと接続ケーブルを介して接続することとした。しかし、ＨＤＤ２の背面側（或いは前面側でもよい。）にＵＳＢ接続端子やＩＥＥＥ１３９４接続端子等の接続端子を設け、この接続端子を介してＨＤＤ２をクライアント端末装置１に接続するようにしてもよい。

【００３６】［クライアント端末装置の電気的構成］次に、図３はクライアント端末装置１のブロック図である。この図３に示すように、クライアント端末装置１は、ＣＰＵ３０と、グラフィックプロセッサ３１（ＧＰＵ）と、ＩＯプロセッサ３２（ＩＯＰ）を有している。

【００３７】また、クライアント端末装置１は、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の光ディスクの再生制御を行う光ディスク制御部３３と、サウンドプロセッサユニット３４（ＳＰＵ）とを有している。

【００３８】また、クライアント端末装置１は、ＣＰＵ３０やＩＯＰ３２が実行するオペレーティングシステムプログラムが格納されたＭＡＳＫ－ＲＯＭ３５と、ＣＰＵ３０のワークエリアや光ディスクから読み出されたデータを一時的に格納するバッファとして機能するＲＡＭ３６とを有している。

【００３９】また、クライアント端末装置１は、光ディスク制御部３３のＲＦアンプ３７を介して供給される光ディスクからの再生出力に対して、例えば誤り訂正処理（ＣＩＲＣ処理）等を施して出力するＣＤ／ＤＶＤＤＳＰ３８を有している。

【００４０】また、クライアント端末装置１は、光ディスク制御部３３のスピンドルモータの回転制御、光ピックアップのフォーカス／トラッキング制御、ディスクトレーのローディング制御等を行うドライバ３９及びメカコントローラ４０を有している。

【００４１】また、クライアント端末装置１は、上記ＰＣカードが接続されるカード型コネクタ４１を有している。

【００４２】これらの各部は、主にバスライン４２，４３等を介してそれぞれ相互に接続されている。

【００４３】なお、ＤＶＤ－ＲＯＭに記憶された映画コンテンツの再生は、メモリカードに記憶されたＤＶＤドライバソウフトウェアに基づいて行われる。或いは、映画コンテンツの再生は、クライアント端末装置１内に内蔵された半導体メモリ４４（DVD Player ROM）に焼き付けられたＤＶＤドライバソウフトウェアに基づいて行われる。

【００４４】ＭＡＳＫ－ＲＯＭ３５には、オペレーティングシステムプログラムが記憶されている。ＣＰＵ３０は、このＭＡＳＫ－ＲＯＭ３５に記憶されているオペレーティングシステムプログラムに基づいて、クライアント端末装置１全体の動作を制御する。

【００４５】また、ＭＡＳＫ－ＲＯＭ３５には、コントローラ接続部７Ａ，７Ｂと、メモリカード装着部８Ａ，８Ｂ、及びカード型コネクタ４１に接続されるコントローラ１４，メモリカード１６及びＨＤＤ２等のハードウェア識別番号（ハードウェアＩＤ）も記憶されている。ＩＯＰ３２は、このＭＡＳＫ－ＲＯＭ３５に記憶されているハードウェアＩＤに基づいて、コントローラ１４，メモリカード１６及びＨＤＤ２等のハードウェアと通信を行い、各接続端子７Ａ，７Ｂ、８Ａ，８Ｂ及びカード型コネクタ４１等に接続されたハードウェアを特定して認識する。

【００４６】なお、ハードウェアＩＤは、クライアント端末装置１全体で一つのＩＤ、メモリカード１６全体で一つのＩＤ、及びＨＤＤ２全体で一つのＩＤ等のように、いわば各ハードウェアに対して総称的に付されたＩＤを意味している。

【００４７】これに対して、後述するクライアントＩＤ，ＭＣ－ＩＤ及びＨＤＤ－ＩＤは、各クライアント端末装置１毎、各メモリカード１６毎、及び各ＨＤＤ２毎にそれぞれ付された各ハードウェア固有のＩＤとなっている。

【００４８】ＧＰＵ３１は、ＣＰＵ３０からの描画指示に従って描画を行い、描画された画像を図示しないフレームバッファに格納する。また、ＧＰＵ３１は、座標変換等の処理を行うジオメトリトランスファエンジンとしての機能を有している。

【００４９】このＧＰＵ３１は、例えば光デイスクに記録されているゲームコンテンツがいわゆる３Ｄグラフィックを利用する場合に、三角形状のポリゴンの集合で仮想的な３次元オブジエクトを構成する。そして、ＧＰＵ３１は、この３次元オブジェクトを仮想的なカメラ装置で撮影することで得られる画像を生成するための諸計算を行う。すなわち、ＧＰＵ３１は、レンダリングを行う場合における透視変換処理（３次元オブジェクトを構成する各ポリゴンの頂点を仮想的なカメラスクリーン上に投影した場合における座標値の計算）等を行う。

【００５０】また、ＧＰＵ３１は、ＣＰＵ３０からの描画指示に従って、必要に応じてジオメトリトランスファエンジンを利用しながら、フレームバッファに対して描画を行う。そして、この描画した画像に対応するビデオ信号（ｖｉｓｕａｌ　ｏｕｔ）を出力する。

【００５１】一方、ＳＰＵ３４は、適応予測符号化された音声データを再生するＡＤＰＣＭ復号機能と、サウンドバッファに記憶されている波形データを再生すること

で、効果音等の音声信号を再生して出力（ａｕｄｉｏ　ｏｕｔ）する再生機能と、サウンドバッファに記憶されている波形データを変調させて再生する変調機能等を備えている。このＳＰＵ３４は、いわゆるサンプリング音源として動作する。ＳＰＵ３４は、ＣＰＵ３０からの指示により、サウンドバッファに記憶されている波形データに基づき楽音，効果音等の音声信号を発生する。

【００５２】このようなクライアント端末装置１は、電源が投入されると、ＣＰＵ３０及びＩＯＰ３２が、ＭＡＳＫ－ＲＯＭ３５からＣＰＵ３０用のオペレーティングシステムプログラム及びＩＯＰ３２用のオペレーティングシステムプログラムをそれぞれ読み出す。

【００５３】ＣＰＵ３０は、ＣＰＵ３０用のオペレーティングシステムプログラムによりクライアント端末装置１の各部を統括的に制御する。ＩＯＰ３２は、ＩＯＰ３２用のオペレーティングシステムプログラムによりコントローラ１４，メモリカード１６、及びＨＤＤ２等との間のデータの入出力を制御する。

【００５４】ＣＰＵ３０は、ＣＰＵ３０用のオペレーティングシステムプログラムに基づいて、動作確認等の初期化処理を行った後、光ディスク制御部３３を制御し、光ディスクに記録されているコンテンツを再生制御する。

【００５５】再生したコンテンツがビデオゲームのゲームコンテンツである場合、ＣＰＵ３０は、ＩＯＰ３２を介してコントローラ１４から受け付けたプレーヤからの指示（コマンド）に従って、ＧＰＵ３１やＳＰＵ３４を制御し、ゲームコンテンツの画像の表示や効果音，楽音等の発声を制御する。

【００５６】再生したコンテンツが映画コンテンツの場合、ＣＰＵ３０は、ＩＯＰ３２を介してコントローラ１４から受け付けたプレーヤからの指示に従って、ＧＰＵ３１やＳＰＵ３４を制御し、映画コンテンツの映像の表示や音声の発声等を制御する。

【００５７】［コピー管理動作］このようなコピー管理システムは、光ディスクに記憶されているコンテンツがＨＤＤ２にコピーされる際に、以下のように管理する。

【００５８】〔インストーラのインストール〕まず、このコピー管理システムは、光ディスクに記憶されているコンテンツをＨＤＤ２にコピーする際に、クライアント端末装置１でコピー制御用のアプリケーションプログラム（インストーラ）を実行する必要がある。この例の場合、インストーラは、コンテンツと共に光ディスクに記憶されている。クライアント端末装置１は、コンテンツのコピー行う前にインストーラのインストールを行う。

【００５９】インストーラのインストールを行う場合、ユーザは、インストーラが記憶されている光ディスクをクライアント端末装置１に装着する。クライアント端末装置１のＣＰＵ３０は、この光ディスクが装着されると自動的に（オートラン）、或いはユーザのコントローラ１４の操作に従って光ディスクに記憶されているインストーラを読み出し、これをメモリカード１６或いはＲＡＭ３６に記憶制御する。

【００６０】このメモリカード１６或いはＲＡＭ３６に記憶されたインストーラは、ユーザが光ディスクに記憶されているコンテンツのコピーを指定した際に、ＣＰＵ３０により実行される。ＣＰＵ３０は、このインストーラを実行することで、コンテンツのコピー制御を行う。

【００６１】なお、インストーラは、システム業者側でインストーラのみ記憶された光ディスクを製造し、これをユーザに配布するようにしてもよい。或いは、システム業者側でインストーラが記憶されたメモリカードを製造し、これをユーザに配布するようにしてもよい。この場合、インストーラのインストール作業を省略可能とすることができる。

【００６２】或いは、インストーラが記憶されたＲＯＭをクライアント端末装置１内に設けてもよい。この場合でも、インストーラのインストール作業を省略可能とすることができる。

【００６３】〔コンテンツの暗号化〕光ディスクに記憶されたコンテンツには、図４に示すように各コンテンツ毎に異なる対称鍵（コンテンツキー：Ｃｏｎｔｅｎｔ－Ｋｅｙ）を用いて暗号化処理が施されている。また、光ディスクには、このように暗号化処理されたコンテンツの他、各光ディスク毎に固有となる「Ｍｅｄｉａ ｕｎｉｑｕｅ ＩＤ（メディアユニークＩＤ：ＭＩＤ）」が記憶されている。

【００６４】〔ユーザ登録〕次に、この第１の実施の形態のコピー管理システムにおいては、光ディスクからＨＤＤ２にコンテンツのコピーを行う場合、各メモリカード１６に固有に付された「メモリカードＩＤ（ＭＣ－ＩＤ）」を用いてシステムサーバ装置４にユーザ登録を行う。このユーザ登録が行われない場合には、コンテンツのコピーは許可されない。

【００６５】図５は、ユーザがシステムサーバ装置４に対してユーザ登録を行うまでの流れを示すフローチャートである。図６は、このユーザ登録によりクライアント端末装置１とシステムサーバ装置４との間で送受信される情報を示す当該コピー管理システムの模式図である。

【００６６】この図５及び図６を用いてユーザ登録動作を説明する。図５のフローチャートは、ユーザがクライアント端末装置１のメイン電源を投入することでスタートとなる。

【００６７】ステップＳ１では、ユーザがインターネット５を介して自分のクライアント端末装置１をシステムサーバ装置４に接続する。

【００６８】具体的には、このクライアント端末装置１には、図１に示したようにインターネット接続用の通信モデム６が接続（或いは内蔵）されている。ユーザによりインターネット接続が指定されると、図３に示すＣＰ

Ｕ３０は、所定のＷＷＷブラウザに基づいて動作し、この通信モデム６を介して当該クライアント端末装置１とシステムサーバ装置４との間の通信回線の確立を図る。これにより、このユーザ登録の行程がステップＳ２に進む。

【００６９】ステップＳ２では、ＣＰＵ３０が、クライアント端末装置１に装着されたメモリカードの識別番号（ＭＣ－ＩＤ），クライアント端末装置１毎に付された固有の識別番号（クライアントＩＤ）及びＨＤＤ２毎に付された固有の識別番号（ＨＤＤ－ＩＤ）をシステムサーバ装置４に送信制御する。

【００７０】具体的には、システムサーバ装置４とクライアント端末装置１との通信回線が確立されると、ＣＰＵ３０は、クライアント端末装置１，ＨＤＤ２及びメモリカード１６とそれぞれ通信を行う。ＣＰＵ３０は、この通信により、クライアント端末装置１に固有に付された識別番号（クライアントＩＤ）、ＨＤＤ２に固有に付された識別番号（ＨＤＤ－ＩＤ）、及びクライアント端末装置１に装着されたメモリカード１６に固有に付された識別番号（ＭＣ－ＩＤ）をそれぞれ取得する。

【００７１】ＣＰＵ３０は、これらの識別番号を、図６に示すようにシステムサーバ装置４側に送信する。これにより、このユーザ登録の行程がステップＳ３に進む。

【００７２】なお、クライアント端末装置１とシステムサーバ装置４との間においては、例えばＳＳＬ（Secure Sockets Layer）等の通信プロトコルに基づいて情報が暗号化されて送受信されるようになっており、通信の安全性が確保されている。

【００７３】また、この例においては、ＣＰＵ３０は、各デバイスと通信を行うことで、クライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤを取得してシステムサーバ装置４側に送信することとした。しかし、クライアント端末装置１，ＨＤＤ２及びメモリカード１６には、クライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤがそれぞれ各筐体にユーザが視認可能なかたちで貼り付けられている。このため、ユーザが、このクライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤを見て、コントローラ１４を操作して手動で各ＩＤの入力を行い、システムサーバ装置４側に送信するようにしてもよい。

【００７４】次に、ステップＳ３では、システムサーバ装置４が、このユーザから送信されたメモリカードの識別番号（ＭＣ－ＩＤ）が有効なＩＤであるか否かを判別する。このユーザ登録行程は、このステップＳ３において、システムサーバ装置４が、ユーザから送信されたＭＣ－ＩＤが有効なＩＤであると判別した場合にステップＳ４に進み、ユーザから送信されたＭＣ－ＩＤが無効なＩＤであると判別した場合にステップＳ７に進む。

【００７５】具体的には、システムサーバ装置４は、全てのクライアント端末装置１のクライアントＩＤ，全てのＨＤＤ２のＨＤＤ－ＩＤ、及び全てのメモリカード１６のＭＣ－ＩＤを記憶したデータベース３を有している。

【００７６】システムサーバ装置４は、ユーザからクライアント端末装置１，ＨＤＤ２及びメモリカード１６の各固有のＩＤが送信されると、まず、ユーザから送信されたメモリカード１６の固有のＩＤであるＭＣ－ＩＤと、データベース３に登録されている各ＭＣ－ＩＤとを照合し、ユーザから送信されたメモリカード１６のＭＣ－ＩＤと同じＭＣ－ＩＤがデータベース３に登録されているか否かを判別する。

【００７７】すなわち、システムサーバ装置４は、ユーザから送信されたメモリカード１６のＭＣ－ＩＤは、データベース３に正規に登録されているＭＣ－ＩＤと同じであるか否かを判別する。

【００７８】ユーザから送信されたメモリカード１６のＭＣ－ＩＤが、データベース３に正規に登録されているいずれのＭＣ－ＩＤとも一致しなかった場合には、システムサーバ装置４は、このユーザ登録のアクセスを、不正なユーザ登録のアクセスと判断する。この場合、システムサーバ装置４は、ステップＳ７において、例えば「このメモリカードではユーザ登録を行うことはできません。」等のユーザ登録を拒否するメッセージをクライアント端末装置１側に返信する（無効通知）。これにより、ユーザ登録が中断されたかたちで、このユーザ登録行程が終了することとなる。

【００７９】一方、ユーザから送信されたメモリカード１６のＭＣ－ＩＤが、データベース３に正規に登録されているいずれかのＭＣ－ＩＤと一致した場合、システムサーバ装置４は、ステップＳ４において、現在、システムサーバ装置４にアクセスしているユーザの固有のＩＤであるユーザＩＤ（Ｕｓｅｒ　ＩＤ）を、例えば乱数等を用いて形成する。

【００８０】そして、システムサーバ装置４は、図６に示すようにそのユーザのクライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤと共に、上記ユーザの固有のＩＤであるユーザＩＤ（Ｕｓｅｒ　ＩＤ）、及び後に説明するＭＣ－Ｋｅｙを一纏めにし、これを「ユーザエントリ情報」としてシステムサーバ装置４のデータベース３に登録する。

【００８１】このように、当該実施の形態のコピー管理システムは、各ユーザが所有するクライアント端末装置１，ＨＤＤ２及びメモリカード１６の３つのＩＤの組み合わせで各ユーザを特定してデータベース３に登録する。

【００８２】クライアント端末装置１，ＨＤＤ２及びメモリカード１６の３つのＩＤが、異なるユーザ間で全て一致するということは有り得ないため、この３つのＩＤに基づいてユーザ登録を行うことにより、ユーザを確実に特定してユーザ登録を行うことができる。これにより、後述する光ディスクに記録されたコンテンツの不正

コピーを、より強力に防止することができる。

【００８３】なお、ユーザ登録の際に、「ＭＣ－ＩＤのみ」、「クライアントＩＤのみ」、「ＨＤＤ－ＩＤのみ」、「ＭＣ－ＩＤとクライアントＩＤ」、「ＭＣ－ＩＤとＨＤＤ－ＩＤ」、或いは「クライアントＩＤとＨＤＤ－ＩＤ」をシステムサーバ装置４側に送信してユーザ登録を行うようにしてもよい。これらの場合でも、各ＩＤはそれぞれ固有のＩＤであるため、異なるユーザ間で重複することはなく、ユーザを略々確実に特定してユーザ登録を行うことができる。

【００８４】次に、ユーザ登録の行程がステップＳ５に進むと、システムサーバ装置４は、ユーザ登録が正規に完了した証として、上記ステップＳ４で形成したユーザエントリ情報のうち、ユーザＩＤ（Ｕｓｅｒ　ＩＤ）をＭＣ－Ｋｅｙで暗号化し、これをクライアント端末装置１側に返信する。

【００８５】〔ＭＣ－Ｋｅｙ〕ここで、上記「ＭＣ－Ｋｅｙ」は、クライアント端末装置１とシステムサーバ装置４との間で送受信する情報を暗号化するための鍵情報である。このＭＣ－Ｋｅｙは、ＭＣ－ＩＤと共にメモリカード１６内に予め記憶されている。

【００８６】ＭＣ－ＩＤは、ユーザが視認可能なようにメモリカード１６の筐体に張り付けられているのであるが、このＭＣ－Ｋｅｙはユーザが視認できないようにメモリカード１６内に記憶されている。また、このＭＣ－Ｋｅｙは、ユーザがメモリカード１６内に記憶されている情報を再生した場合でも、表示や出力が行われることのない秘密性の高い情報となっている。このため、このＭＣ－Ｋｅｙは、ユーザレベルでは、認識することはできないようになっている。

【００８７】また、システムサーバ装置４のデータベース３には、全てのメモリカード１６のＭＣ－ＩＤと共に、各メモリカード１６に記憶されたＭＣ－Ｋｅｙが記憶されている。システムサーバ装置４は、ＭＣ－Ｋｅｙが必要となったときに、このデータベース３からＭＣ－Ｋｅｙを読み出して参照する。このため、クライアント端末装置１からシステムサーバ装置４に対してＭＣ－Ｋｅｙが送信されることはない。

【００８８】このように、ＭＣ－Ｋｅｙは、ユーザレベルでは認識することができず、また、クライアント端末装置１とシステムサーバ装置４との間で送受信されることの無い、秘密性の高い情報となっている。

【００８９】クライアント端末装置１とシステムサーバ装置４との間におけるＭＣ－Ｋｅｙの送受信を不要とすることで、ＭＣ－Ｋｅｙが第三者に傍受される不都合を防止することができる。

【００９０】システムサーバ装置４は、ユーザＩＤ（Ｕｓｅｒ　ＩＤ）を返信する際、予めデータベース３に記憶されているＭＣ－Ｋｅｙの中から、現在アクセスされているユーザのメモリカード１６に対応するＭＣ－Ｋｅｙを選択する。そして、この選択したＭＣ－Ｋｅｙを用いてユーザＩＤ（Ｕｓｅｒ　ＩＤ）を暗号化してクライアント端末装置１に返信する。

【００９１】このＭＣ－Ｋｅｙは、上記ユーザＩＤ（Ｕｓｅｒ　ＩＤ），メディアユニークＩＤ（ｍｅｄｉａ　ｕｎｉｑｕｅ　ＩＤ（ＭＩＤ）），コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）、及びＣｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙをそれぞれ復号化する際に用いられる。

【００９２】ＭＩＤは、各光ディスク毎に固有に付されているＩＤである。コンテンツキーは、光ディスクに記録されたコンテンツを暗号化処理する際に用いられた暗号鍵である。Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙは、ＨＤＤ２にコピーされるコンテンツに対して再暗号化処理を施す際に用いられる暗号鍵である。

【００９３】クライアント端末装置１は、光ディスクから再生したコンテンツを、上記コンテンツキーを用いて復号化する。そして、クライアント端末装置１は、この復号化したコンテンツを、上記Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙを用いて再暗号化処理してＨＤＤ２にコピーするようになっている。詳しくは後述する。

【００９４】次に、ユーザ登録行程がステップＳ６に進むと、クライアント端末装置１が、システムサーバ装置４側から返信されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）をメモリカード１６に記憶制御する。これにより、この図５のフローチャートに示すユーザ登録の全行程が終了する。そして、この時点において、メモリカード１６には、図６に示すように予め記憶されているＭＣ－ＩＤ及びＭＣ－Ｋｅｙと共に、ＭＣ－Ｋｅｙで暗号化されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）が記憶されることとなる。

【００９５】〔メディアユニークＩＤの登録とコンテンツキーの取得〕次に、光ディスクに記録されているコンテンツを何回でもＨＤＤ２にコピー可能とすると、ＭＣ－ＩＤ，ＭＣ－Ｋｅｙ及びユーザＩＤ（Ｕｓｅｒ　ＩＤ）が記録されたメモリカード１６を他のユーザに貸与するだけで、この他のユーザも光ディスクに記録されているコンテンツをこの他のユーザのＨＤＤに不正にコピーすることが可能となり好ましいことではない。

【００９６】このコピー管理システムの場合、コンテンツをＨＤＤ２にコピーする際、ユーザがクライアント端末装置１を介して各光ディスク毎に付された固有のメディアユニークＩＤ（ｍｅｄｉａ　ｕｎｉｑｕｅ　ＩＤ（ＭＩＤ））をシステムサーバ装置４側に送信する。システムサーバ装置４は、ユーザから送信されたメディアユニークＩＤを登録すると共に、暗号化されたコンテンツを復号化するためのコンテンツキーをユーザに送信する。クライアント端末装置１は、光ディスクに記録されているコンテンツを、コンテンツキーを用いて復号化してＨＤＤ２にコピーする。このため、このコンテンツキーを受信するということは、システムサーバ装置４からクライアント端末装置１に対して、コンテンツのコピー

が許諾されたことを意味する。

【００９７】システムサーバ装置４は、クライアント端末装置１から受信したメディアユニークＩＤに対して、過去にコンテンツキーの送信が行われていないことを確認したうえで、コンテンツキーの送信を行う。これにより、同じメディアユニークＩＤに対するコンテンツキーの送信を、１回のみに制限することができる。

【００９８】例えば、あるユーザが自分で購入した光ディスクに記憶されているコンテンツを、自分のＨＤＤ２にコピーした後に、この光ディスクを他のユーザに貸与したとする。他のユーザは、ＨＤＤ２にコンテンツをコピーする際に、貸与された光ディスクのメディアユニークＩＤをシステムサーバ装置４に送信する。

【００９９】しかし、システムサーバ装置４側には、その光ディスクのメディアユニークＩＤに対して、コンテンツキーの送信が行われたことを示す履歴が残っている。この場合、システムサーバ装置４は、他のユーザに対してコンテンツキーの配信は行わない。コンテンツキーを入手することができない他のユーザは、コンテンツをＨＤＤ２にコピーすることはできない。このコピー管理システムは、このようにしてコンテンツの不正コピーを防止している。

【０１００】図７のフローチャートに、メディアユニークＩＤ（ＭＩＤ）の登録とユーザがコンテンツキーを取得するまでの流れを示す。また、図８に、メディアユニークＩＤの登録の際、及びコンテンツキーの取得の際に、クライアント端末装置１とシステムサーバ装置４との間で送受信される各情報を示す。

【０１０１】この図７及び図８を用いてメディアユニークＩＤ（ＭＩＤ）の登録とコンテンツキーの取得動作を説明する。この図７のフローチャートに示すメディアユニークＩＤ（ＭＩＤ）の登録とコンテンツキーの取得行程（登録取得行程）は、ユーザが前述のユーザ登録を正規に終了させていることを前提として実行される。

【０１０２】まず、ステップＳ１１では、クライアント端末装置１が、システムサーバ装置４との間の通信回線の確立を図る。これにより、この登録取得行程がステップＳ１２に進む。

【０１０３】なお、この例においては、前述のユーザ登録終了後に、クライアント端末装置１とシステムサーバ装置４との間で確立された通信回線を一旦切断し、この登録取得行程の実行時に、再度、クライアント端末装置１とシステムサーバ装置４との間の通信回線を確立する説明となっている。

【０１０４】しかし、前述のユーザ登録に続けて、クライアント端末装置１とシステムサーバ装置４との間で確立された通信回線を切断することなく、この登録取得行程を実行するようにしてもよい。この場合、この登録取得行程は、ステップＳ１１をスキップして、スタートからステップＳ１２に進むこととなる。

【０１０５】次にステップＳ１２では、クライアント端末装置１が、前述のように取得したユーザＩＤ（Ｕｓｅｒ　ＩＤ）及びＭＣ－ＩＤをシステムサーバ装置４に送信する。また、クライアント端末装置１は、このユーザＩＤ及びＭＣ－ＩＤと共に、これからＨＤＤ２にコピーするコンテンツが記憶された光ディスクに対して固有に付されているメディアユニークＩＤ（ＭＩＤ）をシステムサーバ装置４側に送信する。

【０１０６】具体的には、ＣＰＵ３０は、メモリカード１６と通信を行い、図８に示すようにＭＣ－ＩＤをシステムサーバ装置４側に送信する。また、ＣＰＵ３０は、前述のようにＭＣ－Ｋｅｙで暗号化されたユーザＩＤをメモリカード１６から読み出してシステムサーバ装置４側に送信する。また、ＣＰＵ３０は、光ディスク制御部３３を制御して光ディスクから再生したメディアユニークＩＤ（ＭＩＤ）をＭＣ－Ｋｅｙで暗号化し、これをシステムサーバ装置４側に送信する。

【０１０７】なお、これらの各情報と共に、クライアントＩＤ及びＨＤＤ－ＩＤをシステムサーバ装置４側に送信するようにしてもよい。クライアントＩＤ及びＨＤＤ－ＩＤは、上記ＭＣ－ＩＤと共にユーザの特定に用いることができる。ＭＣ－ＩＤ，クライアントＩＤ及びＨＤＤ－ＩＤの３つのＩＤを用いてユーザを特定することで、ＭＣ－ＩＤのみでユーザの特定を行う場合よりも、より正確にユーザを特定することができる。

【０１０８】また、クライアント端末装置１とシステムサーバ装置４との間で送受信される情報は、例えばＳＳＬ（Secure Sockets Layer）等の通信プロトコルに基づいて暗号化されて送受信される。これにより、クライアント端末装置１とシステムサーバ装置４との間では、安全性の高い通信を行うことができる。

【０１０９】次に、ステップＳ１３では、システムサーバ装置４が、クライアント端末装置１側から送信されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）が有効なＩＤであるか否かを判別する。このステップＳ１３において、システムサーバ装置４が、ユーザＩＤは有効であると判別した場合、この登録取得行程がステップＳ１４に進む。これに対して、このステップＳ１３において、システムサーバ装置４が、ユーザＩＤは無効であると判別した場合、この登録取得行程はステップＳ１７に進む。

【０１１０】具体的には、システムサーバ装置４は、クライアント端末装置１側から送信されたＭＣ－ＩＤ（及びクライアントＩＤ，ＨＤＤ－ＩＤ）に基づいてデータベース３を参照し、このＭＣ－ＩＤに対応するＭＣ－Ｋｅｙを読み出す。そして、システムサーバ装置４は、このＭＣ－Ｋｅｙに基づいて、ＭＣ－Ｋｅｙで暗号化されて送信されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）及びメディアユニークＩＤ（ＭＩＤ）をそれぞれ復号化する。

【０１１１】前述のように、システムサーバ装置４側のデータベース３には、ユーザエントリ情報としてユーザ

ＩＤ（Ｕｓｅｒ　ＩＤ），ＭＣ－ＩＤ，クライアントＩＤ及びＨＤＤ－ＩＤ等が記憶されている。このため、システムサーバ装置４は、ＭＣ－ＩＤ（クライアントＩＤ及びＨＤＤ－ＩＤ）に基づいてデータベース３内のユーザ情報を検索する。そして、システムサーバ装置４は、このユーザ情報内のユーザＩＤ（Ｕｓｅｒ　ＩＤ）と、現在システムサーバ装置４側にアクセスしてきているユーザのユーザＩＤ（Ｕｓｅｒ　ＩＤ）とを照合する。システムサーバ装置４は、上記両者が一致した場合には、現在システムサーバ装置４側にアクセスしてきているユーザは正規のユーザであると判断する。これにより、この登録取得行程がステップＳ１４に進む。

【０１１２】これに対して、システムサーバ装置４は、データベース３のユーザ情報内のユーザＩＤ（Ｕｓｅｒ　ＩＤ）と、現在システムサーバ装置４側にアクセスしてきているユーザのユーザＩＤ（Ｕｓｅｒ　ＩＤ）とが不一致の場合、そのユーザＩＤ（Ｕｓｅｒ　ＩＤ）は無効と判断する。そして、システムサーバ装置４は、ステップＳ１７において、例えば「ユーザＩＤが無効です。ユーザ登録をして下さい。」等の再度のユーザ登録を促すメッセージをクライアント端末装置１側に返信する（無効通知）。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【０１１３】次に、ステップＳ１４では、システムサーバ装置４が、現在アクセスしてきているユーザの光ディスクに記録されているコンテンツは、過去にコピーされた履歴があるか否かを判別する。

【０１１４】具体的には、このコピー管理システムの場合、データベース３に、各光ディスクにそれぞれ付されているメディアユニークＩＤ（ＭＩＤ）が全て登録されている。システムサーバ装置４は、コンテンツのコピーが行われた際に、データベース３のメディアユニークＩＤ（ＭＩＤ）に対してフラグを立てることで、コピーの履歴を残すようになっている。

【０１１５】このため、システムサーバ装置４は、メディアユニークＩＤ（ＭＩＤ）を復号化すると、そのメディアユニークＩＤ（ＭＩＤ）に対してフラグが立っているか否かを検出する。これにより、そのメディアユニークＩＤ（ＭＩＤ）を有する光ディスクから過去にコンテンツのコピーが行われたか否かを判別することができる。

【０１１６】そのメディアユニークＩＤ（ＭＩＤ）のフラグが立っていない場合、そのメディアユニークＩＤ（ＭＩＤ）が付された光ディスクから過去にコンテンツのコピーは行われていないことを意味する。このため、システムサーバ装置４は、データベース３内におけるそのメディアユニークＩＤ（ＭＩＤ）のフラグを立てる。また、システムサーバ装置４は、このフラグを立てたメディアユニークＩＤ（ＭＩＤ）を、そのユーザのユーザエントリ情報に登録して、この登録取得行程をステップＳ１５に進める。

【０１１７】これに対して、そのメディアユニークＩＤ（ＭＩＤ）のフラグが立っている場合、過去にそのメディアユニークＩＤ（ＭＩＤ）が付された光ディスクからコンテンツのコピーが行われていることを意味する。このため、システムサーバ装置４は、ステップＳ１７において、例えば「このメディアからコンテンツのコピーをすることはできません。」等のコンテンツのコピーを拒否するメッセージをクライアント端末装置１側に返信する（無効通知）。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【０１１８】次にステップＳ１５は、過去に、そのユーザの光ディスクからコンテンツのコピーが行われていない場合に進むステップである。この場合、システムサーバ装置４は、そのユーザのメモリカード１６のＭＣ－Ｋｅｙを用いて、光ディスクに記録されているコンテンツを暗号化したコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の暗号化を行う。そして、この暗号化したコンテンツキーをクライアント端末装置１側に送信する。このコンテンツキーの送信は、システムサーバ装置４側からユーザに対して、光ディスクに記録されているコンテンツのコピーが許可されたことを意味する。

【０１１９】ＭＣ－Ｋｅｙは、そのユーザが所有するメモリカード１６に対して固有に付されている。このため、このコンテンツキーを復号化して使用することができるユーザを、そのＭＣ－Ｋｅｙが記憶されたメモリカード１６を有するユーザのみに限定することができる。従って、上記コンテンツキーを正規のユーザに対してのみ、安全に送信することができる。

【０１２０】また、システムサーバ装置４は、データベース３に記憶されているユーザエントリ情報に基づいて、そのユーザが使用しているクライアント端末装置１のクライアントＩＤ及びＨＤＤ２のＨＤＤ－ＩＤを読み出す。システムサーバ装置４は、これら各ＩＤを、例えば乱数を用いて形成した「コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）」で暗号化してクライアント端末装置１側に返信する。

【０１２１】さらに、システムサーバ装置４は、クライアントＩＤ及びＨＤＤ－ＩＤを暗号化する際に用いたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）を、上記ＭＣ－Ｋｅｙで暗号化してクライアント端末装置１側に返信する。

【０１２２】後に説明するが、クライアント端末装置１は、システムサーバ装置４から返信されたクライアントＩＤと、当該クライアント端末装置１のクライアントＩＤとを照合する。また、クライアント端末装置１は、システムサーバ装置４から送信されたＨＤＤ－ＩＤと、当該クライアント端末装置１に接続されているＨＤＤ２のＨＤＤ－ＩＤとを照合する。そして、クライアント端末装置１は、上記２つのクライアントＩＤと、上記２つの

ＨＤＤ－ＩＤとが、それぞれ一致することを確認してコンテンツのコピーを行うようになっている。

【０１２３】このため、システムサーバ装置４からユーザのクライアント端末装置１に対して、予め登録されているクライアントＩＤ及びＨＤＤ－ＩＤを返信することにより、予めデータベース３に登録されているそのユーザのクライアント端末装置１とＨＤＤ２の組み合わせでのみ、コンテンツのコピー可能とすることができる。

【０１２４】さらに、システムサーバ装置４は、クライアントＩＤ及びＨＤＤ－ＩＤを暗号化したコンテンツジェンキーを、そのユーザが所有するメモリカード１６に固有に付されたＭＣ－Ｋｅｙを用いて暗号化してユーザのクライアント端末装置１に返信する。これにより、コンテンツジェンキーを復号化して使用することができるユーザを、そのＭＣ－Ｋｅｙが記憶されたメモリカード１６を有するユーザのみに限定することができる。従って、上記コンテンツジェンキーを正規のユーザに対してのみ、安全に送信することができる。

【０１２５】次に、ステップＳ１６では、クライアント端末装置１が、システムサーバ装置４側から返信されたＭＣ－Ｋｅｙで暗号化されたコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）、ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）、及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤをそれぞれメモリカード１６に記憶制御する。これにより、この図７のフローチャートに示す登録取得行程が終了する。

【０１２６】このように、このコピー管理システムは、過去にコピー履歴の無いメディアユニークＩＤ（ＭＩＤ）を有する光ディスクに記憶されたコンテンツのみコピーの許可を行う。これにより、各光ディスクに記憶されたコンテンツのコピーを１回に制限することができる。このため、過去にコンテンツのコピーが行われた光ディスクを貸与された第三者は、その貸与された光ディスクからコンテンツのコピーを行うことはできない。従って、１枚の光ディスクから多数のユーザがコンテンツのコピーを行う不正使用を防止することができる。

【０１２７】［コンテンツのコピー］次に、ユーザは、このコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を取得することで、光ディスクに記録されているコンテンツをＨＤＤ２にコピーすることが可能となる。

【０１２８】図９はこのコピー行程の流れを示すフローチャート、図１０はこのコンテンツのコピーが行われる際に、クライアント端末装置１，ＨＤＤ２及びメモリカード１６の間で取り扱う情報を模式的に示した図である。この図９及び図１０を用いてコンテンツのコピー行程の説明を行う。

【０１２９】まず、図９のフローチャートは、前述のメディアユニークＩＤの登録を終了し、コンテンツキーを取得したユーザが、クライアント端末装置１を操作してコンテンツのコピーを指定することでスタートとなる。

【０１３０】ステップＳ２１では、クライアント端末装置１のＩＯＰ３２が、それぞれＭＣ－Ｋｅｙで暗号化されたコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）をメモリカード１６から読み出し、これらをＣＰＵ３０に供給する。

【０１３１】前述のように、ＭＣ－Ｋｅｙは、システムサーバ装置４及びこのクライアント端末装置１でそれぞれ保持している。このため、ＣＰＵ３０は、この保持しているＭＣ－Ｋｅｙを用いて、上記暗号化されているコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）を復号化処理する。そして、ＣＰＵ３０は、この復号化したコンテンツキー及びコンテンツジェンキーをＲＡＭ３６に記憶制御する。これにより、このコピー行程がステップＳ２２に進む。

【０１３２】ステップＳ２２では、ＩＯＰ３２が、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤをメモリカード１６から読み出し、これらをＣＰＵ３０に供給する。ＣＰＵ３０は、先に復号化したコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）を用いてこのクライアントＩＤ及びＨＤＤ－ＩＤを復号化する。

【０１３３】また、このステップＳ２２では、ＣＰＵ３０が、上記復号化したクライアントＩＤと当該クライアント端末装置１に付されたクライアントＩＤとを照合する。また、ＣＰＵ３０は、上記復号化したＨＤＤ－ＩＤと、当該クライアント端末装置１に接続されたＨＤＤ２のＨＤＤ－ＩＤとを照合する。

【０１３４】次に、ステップＳ２３では、ＣＰＵ３０が、上記各クライアントＩＤ、及び上記各ＨＤＤ－ＩＤがそれぞれ一致するか否かを判別する。両者が一致する場合はコンテンツのコピーを実行すべくこのコピー行程がステップＳ２４に進む。両者が不一致の場合はこのコピー行程がステップＳ２８に進む。

【０１３５】メモリカード１６から復号化されたクライアントＩＤ及びＨＤＤ－ＩＤが、そのクライアント端末装置１のクライアントＩＤ及びＨＤＤ－ＩＤと一致しないということは、前述のコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得が、正規のユーザのクライアント端末装置１及びＨＤＤ２に基づいて行われていないことを示す。

【０１３６】すなわち、この場合、正規ユーザからメモリカード１６を貸与された不正ユーザが、コンテンツのコピーを行おうとしていることを示している。

【０１３７】このため、ＣＰＵ３０は、例えば「コピーを行うことはできません。」等のコンテンツのコピーを拒否するメッセージをユーザに対して表示制御する。こ

れにより、中断されたかたちでこのコピー行程が終了することとなる。

【０１３８】次に、ステップＳ２４は、クライアント端末装置１が、上記各クライアントＩＤ及び上記各ＨＤＤ－ＩＤの一致を検出した際に実行するステップである。この場合、ＣＰＵ３０は、光ディスク制御部３３により光ディスクから再生されたコンテンツを、ＲＡＭ３６に記憶されているコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を用いて復号化する。また、ＣＰＵ３０は、この復号化したコンテンツを、ＲＡＭ３６に記憶されているコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で再暗号化してＨＤＤ２に供給する。

【０１３９】次に、ステップＳ２５では、ＨＤＤ２が、図１０に示すように上記コンテンツジェンキーで再暗号化されたコンテンツをハードディスクに保存（コピー）する。

【０１４０】次に、ステップＳ２６ではクライアント端末装置１のＣＰＵ３０がＨＤＤ２と通信を行うことで、コンテンツのコピーが完了したか否かを判別する。コピーが完了していない場合、ＣＰＵ３０は、前述のステップＳ２４及びステップＳ２５の動作を繰り返し実行制御することで、コンテンツのコピーが完了するまでの間、ＨＤＤ２に対してコンテンツの供給を行う。コンテンツのコピーが完了すると、このコピー行程がステップＳ２７に進む。

【０１４１】ステップＳ２７では、コンテンツのコピーが完了したため、ＩＯＰ３２が、メモリカード１６に記憶されているコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を消去する。これにより、このコピー行程が終了する。

【０１４２】このように、クライアント端末装置１は、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）で暗号化されて光ディスクに記憶されているコンテンツを、システムサーバ装置４から発行されたコンテンツキーで復号化してＨＤＤ２にコピーする。そして、このコンテンツのコピー後に、メモリカード１６内に記憶されているコンテンツキー（システムサーバ装置４から発行されたコンテンツキー）を消去する。

【０１４３】前述のように、過去にコンテンツのコピーが行われた光ディスクに対しては、データベース３にコピー履歴が残るため、システムサーバ装置４は、原則的にコンテンツキーの再発行は行わない。このため、一度コンテンツのコピーが行われた光ディスクを貸与された第三者からのコピー申請は、システムサーバ装置４が、上記データベースのコピー履歴に基づいて拒否する。そして、システムサーバ装置４は、この第三者に対しては、コンテンツキーを送信しない。

【０１４４】上記第三者は、コンテンツキーを取得することができないため、貸与された光ディスクに記憶されているコンテンツを復号化することができない。このため、上記第三者がコンテンツをＨＤＤ等の二次記憶媒体にコピーすることができたとしても、コンテンツを復号化することができないことから、該コンテンツを使用することができない。従って、このコピー管理システムは、コンテンツの不正使用を防止することができる。

【０１４５】［コピーされたコンテンツの再生］次に、このようにＨＤＤ２にコピーされたコンテンツは、ユーザが繰り返し再生して利用することができるようになっている。

【０１４６】図１１に、ＨＤＤ２に保存されたコンテンツの再生行程の流れを示すフローチャートを示す。また、図１２にこの再生行程において、クライアント端末装置１，ＨＤＤ２及びメモリカード１６の間で取り扱われる情報の模式図を示す。

【０１４７】図１１のフローチャートは、前述のコンテンツのコピーを正規に終了させたユーザが、コンテンツの再生を指定することでスタートとなる。

【０１４８】ステップＳ３１では、クライアント端末装置１のＩＯＰ３２が、上記ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）をメモリカード１６から読み出し、これをＣＰＵ３０に供給する。ＣＰＵ３０は、このコンテンツジェンキーを、クライアント端末装置１側で保持しているＭＣ－Ｋｅｙを用いて復号化して再生する。

【０１４９】次に、ステップＳ３２では、ＩＯＰ３２が、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤをメモリカード１６から読み出し、これをＣＰＵ３０に供給する。ＣＰＵ３０は、先に復号化したコンテンツジェンキーを用いて、この暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤを復号化する。

【０１５０】次に、ステップＳ３３では、ＣＰＵ３０が、当該クライアント端末装置１に付されているクライアントＩＤと、上記コンテンツジェンキーで復号化したクライアントＩＤとを照合する。

【０１５１】また、ＣＰＵ３０は、当該クライアント端末装置１に接続されているＨＤＤ２のＨＤＤ－ＩＤと、上記コンテンツジェンキーで復号化したＨＤＤ－ＩＤとを照合する。

【０１５２】上記各クライアントＩＤ及び上記各ＨＤＤ－ＩＤが一致しないということは、他のユーザのメモリカード１６，他のユーザのクライアント端末装置１、或いは他のユーザのＨＤＤ２が用いられていることを示す。このため、ＣＰＵ３０は、ステップＳ３５において、例えば「コンテンツを再生することはできません。」等のコンテンツの再生を拒否するメッセージをユーザに表示する。これにより、中断されるかたちでこのコンテンツの再生行程が終了することとなる。

【０１５３】このように、このコピー管理システムにおいては、ＨＤＤ２にコピーされたコンテンツを再生する

際にも、クライアントＩＤ及びＨＤＤ－ＩＤの照合を行う。例えば、正規のユーザが所有するメモリカード１６とコンテンツが保存されたＨＤＤ２が、第三者に貸与された場合を考える。第三者は、自分のクライアント端末装置に対して、この貸与されたメモリカード１６とＨＤＤ２を接続して、該ＨＤＤ２内に記憶されているコンテンツの再生を行うこととなる。

【０１５４】しかし、メモリカード１６内に記憶されているクライアントＩＤは、正規のユーザのクライアントＩＤである。このため、第三者のクライアント端末装置のクライアントＩＤと、メモリカード１６に記憶されているクライアントＩＤとが一致しないことから、第三者のクライアント端末装置において、ＨＤＤ２に記憶されているコンテンツの再生は拒否される。このため、メモリカード１６とＨＤＤ２が貸与された場合でも、ＨＤＤ２にコピーされているコンテンツの使用を防止することができる。

【０１５５】次に、上記各クライアントＩＤ及び上記各ＨＤＤ２がそれぞれ一致した場合、ＣＰＵ３０は、先に復号化したコンテンツジェンキーを用いてＨＤＤ２のコンテンツを復号化し、これをＲＡＭ３６に記憶する。これにより、このコンテンツの再生行程が終了する。

【０１５６】ＲＡＭ３６に記憶されたコンテンツが、例えばビデオゲームのゲームコンテンツであった場合、ＣＰＵ３０は、このゲームコンテンツに基づいて動作する。そして、ＣＰＵ３０は、例えばビデオゲームのキャラクタを表示制御し、効果音やＢＧＭ等を発音制御する。これにより、ユーザは、光ディスクからＨＤＤ２にコピーしたゲームコンテンツに基づいてビデオゲームを楽しむことができる。

【０１５７】光ディスクからゲームコンテンツを直接的に再生してビデオゲームを行う場合、新たなビデオゲームを行う毎に光ディスクの着脱作業が必要である。しかし、このように各光ディスクに記録されたゲームコンテンツをＨＤＤ２にコピーしておくことにより、新たなビデオゲームを行う毎に必要となっていた光ディスクの着脱作業を省略することができる。このため、新たなビデオゲームをスムーズに開始可能とすることができる。

【０１５８】なお、光ディスクからコンテンツのコピーが終了した後には、メモリカード１６に記憶されているコンテンツキーが消去されるため、コンテンツの再コピーは行うことができない。しかし、メモリカード１６に記憶されているコンテンツジェンキーは、コピー完了後も消去されることはない。このため、コンテンツジェンキーで暗号化されてＨＤＤ２にコピーされたコンテンツは、このメモリカード１６に記憶されているコンテンツジェンキーを用いて繰り返し復号化して再生可能である。

【０１５９】［デバイスの修理，交換に対する対応］次に、このコピー管理システムの場合、システムサーバ装置４は、クライアントＩＤ，ＨＤＤ－ＩＤ，ＭＣ－ＩＤ等（以下、一括してデバイスＩＤという）と、ユーザＩＤとをユーザエントリ情報として一括して管理する。しかし、クライアント端末装置１やＨＤＤ２等のデバイスを破損等により交換した場合、この交換したデバイスのデバイスＩＤが、ユーザエントリ情報として登録されているデバイスＩＤとは異なるものとなる。従って、デバイスの交換を行うと、正規のユーザであるにも拘わらず、その交換したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【０１６０】一方、このコピー管理システムの場合、デバイスＩＤの固有性を確保することでコンテンツの不正使用を防止するようになっている。このため、クライアント端末装置１やＨＤＤ２等のデバイスを修理により復元した場合でも、この修理後のデバイスに対して、修理前に付されていたデバイスＩＤとは異なる新たなデバイスＩＤを付し、修理前のデバイスと修理後のデバイスとを明確に区別して管理することが好ましい。

【０１６１】ただ、このように修理後のデバイスに対して新たなデバイスＩＤを付すと、前述のデバイスの交換時と同様に、正規のユーザであるにも拘わらず、その修理したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【０１６２】このコピー管理システムは、デバイスの修理及び交換により新たなデバイスＩＤを用いることで懸念される上記不都合を、以下のように防止している。

【０１６３】〔クライアント端末装置及びＨＤＤの修理，交換に対する対応〕図１３に、このコピー管理システムにおけるクライアント端末装置及びＨＤＤの修理，交換に対する対応を説明するための模式図を示す。この図１３中、×印が描かれているクライアント端末装置１或いはＨＤＤ２は、破損したデバイスを示している。

【０１６４】この図１３において、デバイスが破損した場合、ユーザは、その破損したデバイスを、メモリカード１６と共に、このコピー管理システムを管理する管理者側のリペアセンターに送付する。

【０１６５】すなわち、この場合メモリカード１６は破損していないのであるが、メモリカード１６にはコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）やコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤ（以下、各ＩＤを一括してデバイスＩＤという）が記憶されている。このため、デバイスが破損した場合でも、この破損したデバイスと共にメモリカード１６を上記リペアセンターに送付（或いは持ち込み）するようになっている。

【０１６６】リペアセンターでは、故障したデバイスが送付されると、このデバイスが正常に動作するように修理，交換等すると共に、この修理，交換等したデバイスに対して新たなデバイスＩＤを付与する。

【０１６７】具体的には、クライアント端末装置１のクライアントＩＤは、例えば上記ハードウェアＩＤやオペレーティングシステムプログラムと共にＭＡＳＫ－ＲＯＭ３５に記憶されている。また、ＨＤＤ２内にも上記ＭＡＳＫ－ＲＯＭ３５と同様のＭＡＳＫ－ＲＯＭが設けられており、ＨＤＤ－ＩＤは、このＭＡＳＫ－ＲＯＭに記憶されている。このため、リペアセンターでは、デバイスの修理を行った場合には、この修理を行う前に設けられていたＭＡＳＫ－ＲＯＭを取り外し、新たなクライアントＩＤ或いはＨＤＤ－ＩＤが記憶されたＭＡＳＫ－ＲＯＭに交換することで、新たなクライアントＩＤ或いはＨＤＤ－ＩＤの付与を行う。

【０１６８】なお、デバイス自体を新品のデバイスに交換する場合は、この新品のデバイスのＭＡＳＫ－ＲＯＭ内に、故障したデバイスとは異なるデバイスＩＤが記憶されているため、上記修理時のようなＭＡＳＫ－ＲＯＭの交換は行わない。

【０１６９】次に、リペアセンターのオペレータは、故障したデバイスと共に送付されたメモリカード１６のＭＣ－ＩＤを再生する。オペレータは、リペアセンターに設けられている端末装置を介して上記システムサーバ装置４のデータベース３にアクセスし、上記メモリカード１６から再生したＭＣ－ＩＤに基づいて、上記データベース３に記憶されているユーザエントリ情報を参照する。そして、オペレータは、端末装置を操作して、このデータベース３に記憶されているユーザエントリ情報のうち、デバイスＩＤを、新たに付与したデバイスＩＤに修正登録する。また、オペレータは、端末装置を介してデータベース３を操作し、コピー済みのコンテンツに対して立てられている上記フラグを降ろす。

【０１７０】また、オペレータは、端末装置を操作して、メモリカード１６内に記憶されている、ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）と、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたデバイスＩＤ（クライアントＩＤ及びＨＤＤ－ＩＤ）とをそれぞれ消去する。そして、このメモリカード１６を、修理，交換等したデバイスと共にユーザに返送（或いは手渡し）する。

【０１７１】これにより、ユーザのデバイス（クライアント端末装置１，ＨＤＤ２及びメモリカード１６）の状態は、図５及び図６を用いて説明したユーザ登録行程が終了した直後の状態（＝コンテンツのコピーを行う直前の状態）に戻ることとなる。

【０１７２】このメモリカード１６とデバイスが返送されたユーザは、図７及び図８を用いて説明したメディアユニークＩＤ（ＭＩＤ）の登録とコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得を再度行うようにクライアント端末装置１を操作する。

【０１７３】クライアント端末装置１は、ユーザの操作に対応してシステムサーバ装置４にアクセスし、メディアユニークＩＤ（ＭＩＤ）の登録を行う。そして、クライアント端末装置１は、この登録によりシステムサーバ装置４から取得したコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を用いて光ディスクに記憶されているコンテンツをＨＤＤ２に再コピーする。

【０１７４】これにより、デバイスの修理や交換によりデバイスＩＤを新たに付与した場合でも、正規のユーザであれば、新たなデバイスＩＤに基づいてコンテンツのコピーや再生を実行可能とすることができる。

【０１７５】また、コピー管理システム側では、修理や交換により復元したデバイスに対して新たなデバイスＩＤを付すことにより、修理前のデバイスと修理後のデバイスとを明確に区別して管理することができる。

【０１７６】〔メモリカードの破損，紛失に対する対応〕次に、このコピー管理システムの場合、メモリカード１６の破損、或いは紛失に対しては、以下のように対処する。図１４に、このコピー管理システムにおけるメモリカード１６の破損，紛失に対する対応を説明するための模式図を示す。この図１４中、点線の枠で囲んで示すメモリカード１６が、破損或いは紛失したメモリカード１６を示している。

【０１７７】メモリカード１６が破損或いは紛失した場合、ユーザは、この図１４に示すように、インターネット５を介してクライアント端末装置１をシステムサーバ装置４に接続し、システムサーバ装置４に対してメモリカードの再発行を申請する。

【０１７８】この申請がなされるとシステムサーバ装置４は、ユーザＩＤの入力画面データをクライアント端末装置１側に送信する。これにより、ユーザのクライアント端末装置１は、テレビジョン受像機１８にユーザＩＤの入力画面を表示制御する。

【０１７９】ユーザは、この入力画面に対してユーザＩＤの入力を行う。しかし、この場合、メモリカード１６が破損或いは紛失しているため、メモリカード１６からユーザＩＤ（Ｕｓｅｒ　ＩＤ）を読み出すことはできない。このため、ユーザは、ユーザＩＤが発行された際にメモ帳等に書き写しておいたユーザＩＤを見て、ユーザＩＤの入力を行う。クライアント端末装置１は、この入力されたユーザＩＤをシステムサーバ装置４に送信する。

【０１８０】次にシステムサーバ装置４は、このユーザから送信されたユーザＩＤに対応するユーザエントリ情報をデータベース３から参照する。これにより、システムサーバ装置４は、破損或いは紛失したメモリカード１６のＭＣ－ＩＤ及びＭＣ－Ｋｅｙと共に、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）やそのメモリカード１６でコピーされたコンテンツ等を認識することができる。

【０１８１】次に、システムサーバ装置４は、新たなＭ

Ｃ－ＩＤを有するメモリカード１６ｎｅｗに対して、新たなＭＣ－Ｋｅｙ（ＮｅｗーＭＣ－Ｋｅｙ）と、このＮｅｗーＭＣ－Ｋｅｙで新たに暗号化したコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）と、このコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化したクライアントＩＤ及びＨＤＤ－ＩＤを記録し直す。また、システムサーバ装置４は、データベース３に記憶されているユーザエントリ情報が、この新たなメモリカード１６Ｎｅｗに対応したユーザエントリ情報となるように、ＭＣ－ＩＤやＭＣ－Ｋｅｙ等の書き換えを行う。

【０１８２】なお、この場合、メモリカード１６が破損或いは紛失した場合であり、ユーザのクライアント端末装置１及びＨＤＤ２は正常に動作している。このため、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されるクライアントＩＤ及びＨＤＤ－ＩＤとしては、元のデバイスＩＤがそのまま用いられる。

【０１８３】次に、リペアセンターは、このメモリカード１６ｎｅｗを、例えば郵送等によりユーザ側に物理的に送付する。前述のように、システムサーバ装置４側ではこのメモリカード１６ｎｅｗ内の各情報の書き換えと共に、データベース３のユーザエントリ情報の書き換えを行っている。このため、送付されたメモリカード１６ｎｅｗを受け取ったユーザは、このメモリカード１６ｎｅｗ，クライアント端末装置１及びＨＤＤ２の組み合わせのシステムを用いて、以前と同様に、コンテンツのコピーや、コピーしたコンテンツの再生等を行うことができる。

【０１８４】［第１の実施の形態の効果］以上の説明から明らかなように、この第１の実施の形態のコピー管理システムは、システム管理者が、コンテンツキーで暗号化処理を施したコンテンツを、メディアユニークＩＤ（ＭＩＤ）が付された光ディスクに記憶させてユーザに配布する。

【０１８５】ユーザは、コンテンツのコピーを行う際に、システムサーバ装置４に対して光ディスクのＭＩＤを送信する。また、ユーザは、自分が使用しているデバイスのデバイスＩＤ（クライアントＩＤ，ＨＤＤ－ＩＤ，ＭＣ－ＩＤ等）をシステムサーバ装置４に送信する。

【０１８６】システムサーバ装置４は、各ユーザが使用しているデバイスのデバイスＩＤに関連付けて、過去にコンテンツのコピーが行われた光ディスクのＭＩＤをデータベース３に記憶している。

【０１８７】システムサーバ装置４は、ユーザからコンテンツのコピー申請がなされた際に、ユーザが使用しているデバイスＩＤと光ディスクのＭＩＤ基づいてデータベース３を参照する。システムサーバ装置４は、データベース３内に同じＭＩＤが登録されていないことを条件として、コンテンツを復号化するためのコンテンツキーを、ユーザのクライアント端末装置１に送信する。

【０１８８】クライアント端末装置１は、このコンテンツキーを用いて光ディスクに記憶されているコンテンツを復号化してＨＤＤ２にコピーする。

【０１８９】このコピー管理システムは、データベース３内に登録されているＭＩＤと同じＭＩＤを掲示してコピー申請がなされた場合は、上記コンテンツキーの配信は行われない。このため、このコピー管理システムは、コンテンツのコピーを１回に制限することができ、コンテンツの不正コピーを防止することができる。

【０１９０】［第２の実施の形態］次に本発明の第２の実施の形態となるコピー管理システムの説明をする。上述の第１の実施の形態のコピー管理システムは、ユーザが自分のクライアント端末装置１をシステム管理者側のシステムサーバ装置４に直接的に接続してユーザ登録を行い、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）等を取得してコンテンツのコピーを行うものであった。

【０１９１】この第２の実施の形態のコピー管理システムは、ユーザのクライアント端末装置１とシステム管理者側のシステムサーバ装置４との間に、第３者が管理する第３者管理サーバ装置が設けられている。ユーザはこの第３者管理サーバ装置を介してコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）等の取得を行う。第３者管理サーバ装置は、このコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）等の提供に対する課金を行う。

【０１９２】［第２の実施の形態の構成］図１５に、この第２の実施の形態となるコピー管理システムのシステム構成図を示す。この図１５は、光ディスクからコンテンツをコピーする際にコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を取得する流れを示している。

【０１９３】この図１５において、システムサーバ装置４と第３者管理サーバ装置５０とは、例えば専用回線や、公衆回線を専用回線のように利用可能なＶＰＮ（VirtualPrivate Network）等により相互に接続されている。

【０１９４】また、システムサーバ装置４はインターネット５には接続されておらず、この第３者管理サーバ装置５０がインターネット５に接続されている。このため、ユーザは、システムサーバ装置４に対して直接的にアクセスすることはできず、この第３者管理サーバ装置５０を介して間接的にシステムサーバ装置４にアクセスすることとなる。

【０１９５】［第２の実施の形態の動作］次に、この第２の実施の形態のコピー管理システムの動作説明をする。この第２の実施の形態のコピー管理システムの場合、光ディスクからコンテンツのコピーを行おうとするユーザは、インターネット５を介して自分のクライアント端末装置１を第３者管理サーバ装置５０に接続する。そして、ユーザは、クライアント端末装置１を介して、ＭＣ－ＩＤ，ユーザＩＤ（Ｕｓｅｒ　ＩＤ），メディア

ユニークＩＤ（ＭＩＤ）を第３者管理サーバ装置５０側に送信する。また、ユーザは、クライアント端末装置１を介して、第３者管理サーバ装置５０用のアカウント情報（例えばユーザ名やパスワード等）を第３者管理サーバ装置５０に送信する。

【０１９６】クライアント端末装置１は、ＭＣ－ＩＤ及びアカウント情報をそのまま第３者管理サーバ装置５０に送信する。また、クライアント端末装置１は、ユーザＩＤ（Ｕｓｅｒ　ＩＤ）及び光ディスクのメディアユニークＩＤ（ＭＩＤ）をＭＣ－Ｋｅｙで暗号化し、これらを第３者管理サーバ装置５０に送信する。

【０１９７】第３者管理サーバ装置５０は、クライアント端末装置１から送信された各情報のうち、アカウント情報を抽出して取得する。また、第３者管理サーバ装置５０は、専用回線（或いは上記ＶＰＮ）を介してＭＣ－ＩＤ，ＭＣ－Ｋｅｙで暗号化されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）、及びＭＣ－Ｋｅｙで暗号化されたメディアユニークＩＤ（ＭＩＤ）をシステムサーバ装置４に送信する。

【０１９８】システムサーバ装置４は、このＭＣ－ＩＤ，ユーザＩＤ及びＭＩＤを受信すると、前述と同様に暗号化されて光ディスクに記録されているコンテンツを復号化するためのコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）をＭＣ－Ｋｅｙで暗号化して第３者管理サーバ装置５０に返信する。また、システムサーバ装置４は、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）をＭＣ－Ｋｅｙで暗号化して第３者管理サーバ装置５０に返信する。さらにシステムサーバ装置４は、このコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）でユーザのクライアントＩＤ及びＨＤＤ－ＩＤを暗号化して第３者管理サーバ装置５０に返信する。

【０１９９】第３者管理サーバ装置５０は、このＭＣ－Ｋｅｙで暗号化されたコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ），ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）、及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたユーザのクライアントＩＤ，ＨＤＤ－ＩＤを、それぞれインターネット５を介してユーザのクライアント端末装置１に転送する。

【０２００】第３者管理サーバ装置５０は、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を提供した代償として、先にクライアント端末装置１から送信された第３者管理サーバ装置５０用のアカウント情報に基づいて、そのユーザに対する課金を行う。

【０２０１】クライアント端末装置１は、第３者管理サーバ装置５０から送信された上記コンテンツキー，コンテンツジェンキー、クライアントＩＤ、及びＨＤＤ－ＩＤをメモリカード１６に記憶制御して、前述のようにコンテンツのコピー、及びコピーしたコンテンツの再生に用いる。

【０２０２】第３者管理サーバ装置５０側には、例えばユーザのクレジットカードの番号や、プリペイドされた金額情報が予め登録されている。このため、第３者管理サーバ装置５０は、コンテンツキーの提供と引き替えに課金した金額をクレジットカード会社に請求して回収する。或いは第３者管理サーバ装置５０は、プリペイドされている残金から課金分の金額を減算して回収する。

【０２０３】このように回収された金銭は、例えばシステムサーバ装置４の管理者と第３者管理サーバ装置５０の管理者との間において、所定の割合で分配されることとなる。

【０２０４】［第２の実施の形態の効果］このようにこの第２の実施の形態のコピー管理システムは、クライアント端末装置１とシステムサーバ装置４との間に第３者管理サーバ装置５０を設けて構成する。ユーザはこの第３者管理サーバ装置５０を介してシステムサーバ装置４にアクセスしてコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の配布を請求する。第３者管理サーバ装置５０は、このコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）をユーザに配布して課金を行う。

【０２０５】これにより、このコピー管理システムは、第３者（第３者管理サーバ装置５０の管理者）が介在するコピー管理システムという新規なコピー管理システムを提供することができる他、上述の第１の実施の形態のコピー管理システムと同じ効果を得ることができる。

【０２０６】また、このコピー管理システムは、コンテンツキーをユーザに配布した際に課金を行うことで、光ディスク等を介して、或いは所定のネットワークを介してコンテンツを無償でユーザに配布することができる。

【０２０７】なお、このコピー管理システムにおいて、光ディスクにＭＩＤを付すことなくユーザに配布し、ユーザからコピーの申請があった際に、システムサーバ装置４或いは第３者管理サーバ装置５０が、そのユーザに対してコンテンツキーを配布して課金を行うようにしてもよい。

【０２０８】また、この第２の実施の形態のコピー管理システムは、第３者管理サーバ装置５０が課金を行うこととしたが、これは、システムサーバ装置４が課金を行うようにしてもよい。

【０２０９】最後に、本発明は一例として説明した上述の各実施の形態に限定されることはない。このため、上述の各実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。

【０２１０】例えば、上述の各実施の形態の説明では、クライアント端末装置１は、デバイス識別情報として、クライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤをシステムサーバ装置４に送信することとした。しかし、クライアント端末装置１からクライアントＩＤのみをシステムサーバ装置４に送信してもよい。同様に、クライアン

ト端末装置１からＨＤＤ－ＩＤのみをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からＭＣ－ＩＤのみをシステムサーバ装置４に送信してもよい。

【０２１１】また、クライアント端末装置１からクライアントＩＤ及びＨＤＤ－ＩＤをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からクライアントＩＤ及びＭＣ－ＩＤをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からＨＤＤ－ＩＤ及びＭＣ－ＩＤをシステムサーバ装置４に送信してもよい。

【０２１２】すなわち、上述の各実施の形態のコピー管理システムは、システムサーバ装置４側で、コンテンツのコピーが行われる記憶媒体と、コンテンツのコピーに使用されるデバイスとを関連付けてコピー管理を行うことで不正コピーを防止する。このため、クライアント端末装置１からシステムサーバ装置４に送信されるデバイス識別情報としては、ユーザを特定可能な識別情報であればよい。

【０２１３】また、上述の各実施の形態の説明では、メモリカード１６を用いることとしたが、このコピー管理システムの場合、必ずしもメモリカード１６は必要としない。メモリカード１６を用いない場合は、メモリカード１６に記憶される上記コンテンツキーやコンテンツジェンキー等は、ＨＤＤ２やクライアント端末装置１に内蔵されているメモリに記憶させればよい。

【０２１４】

【発明の効果】本発明は、記憶媒体の持ち主である正規のユーザに対してのみ、記憶媒体に記憶されたコンテンツのコピーを許可することができる。このため、記憶媒体に記憶されたコンテンツの不正コピーを防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態のコピー管理システムのシステム構成を示すブロック図である。

【図２】コピー管理システムを構成するクライアント端末装置及びハードディスクドライブ（ＨＤＤ）の外観を示す斜視図である。

【図３】クライアント端末装置の電気的な構成を示すブロック図である。

【図４】コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）で暗号化されたデジタルコンテンツが記憶された、このコピー管理システムに用いられる光ディスクを説明するための図である。

【図５】コピー管理システムにおけるユーザ登録の流れを示すフローチャートである。

【図６】ユーザ登録時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

【図７】コピー管理システムにおける、光ディスクに個別に付されたメディアユニークＩＤ（ＭＩＤ）の登録動作と、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得動作を示すフローチャートである。

【図８】光ディスクに個別に付されたメディアユニークＩＤ（ＭＩＤ）の登録時、及びコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

【図９】コピー管理システムにおけるコピー行程の流れを示すフローチャートである。

【図１０】コピー実行時にクライアント端末装置，メモリカード及びハードディスクドライブの間で送受信される各情報を示す模式図である。

【図１１】コピー管理システムにおける、ハードディスクドライブにコピーしたデジタルコンテンツの再生動作を示すフローチャートである。

【図１２】ハードディスクドライブにコピーしたデジタルコンテンツの再生時に、クライアント端末装置，メモリカード及びハードディスクドライブの間で送受信される情報を示す模式図である。

【図１３】クライアント端末装置或いはハードディスクドライブの修理或いは交換に対するコピー管理システムの対応を説明するための模式図である。

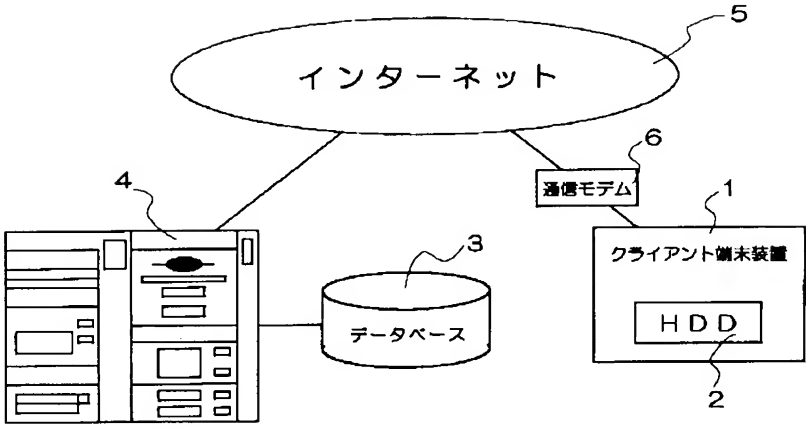
【図１４】メモリカードの破損或いは紛失に対するコピー管理システムの対応を説明するための模式図である。

【図１５】光ディスクに個別に付されたメディアユニークＩＤ（ＭＩＤ）の登録時、及びコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示す、本発明の第２の実施の形態となるコピー管理システムの模式図である。

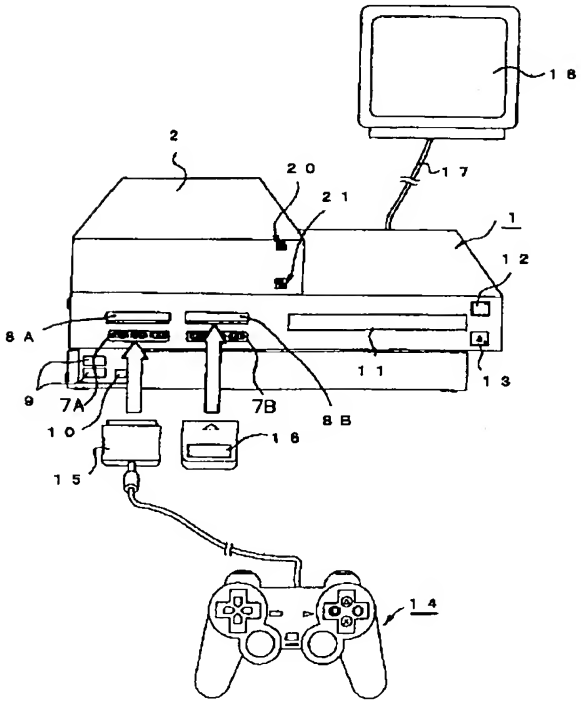
【符号の説明】

１…クライアント端末装置、２…ハードディスクドライブ（ＨＤＤ），３…データベース，４…システムサーバ装置，５…インターネット，６…通信モデム

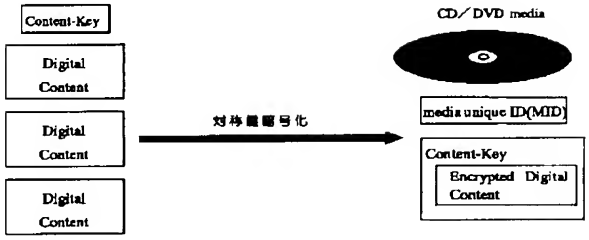
【図１】


インターネット
5
6
通信モデム
4
1
クライアント端末装置
3
データベース
HDD
2

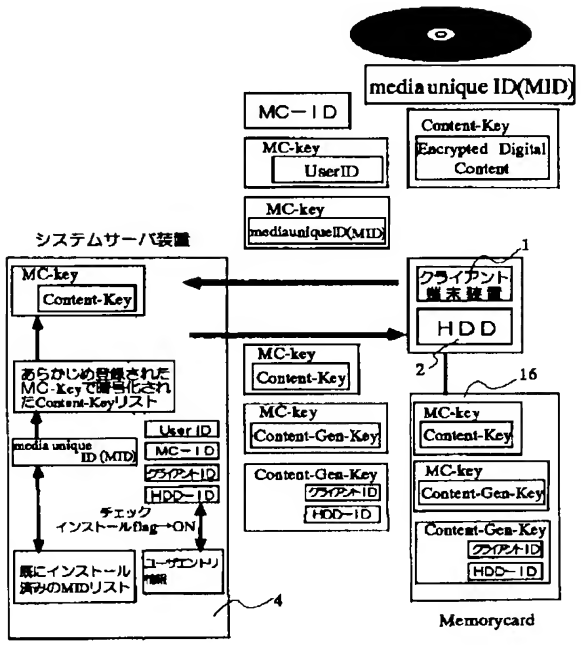
【図２】


18
2
20
17
21
1
12
8A
11
13
9
7A
7B
8B
10
16
15
14

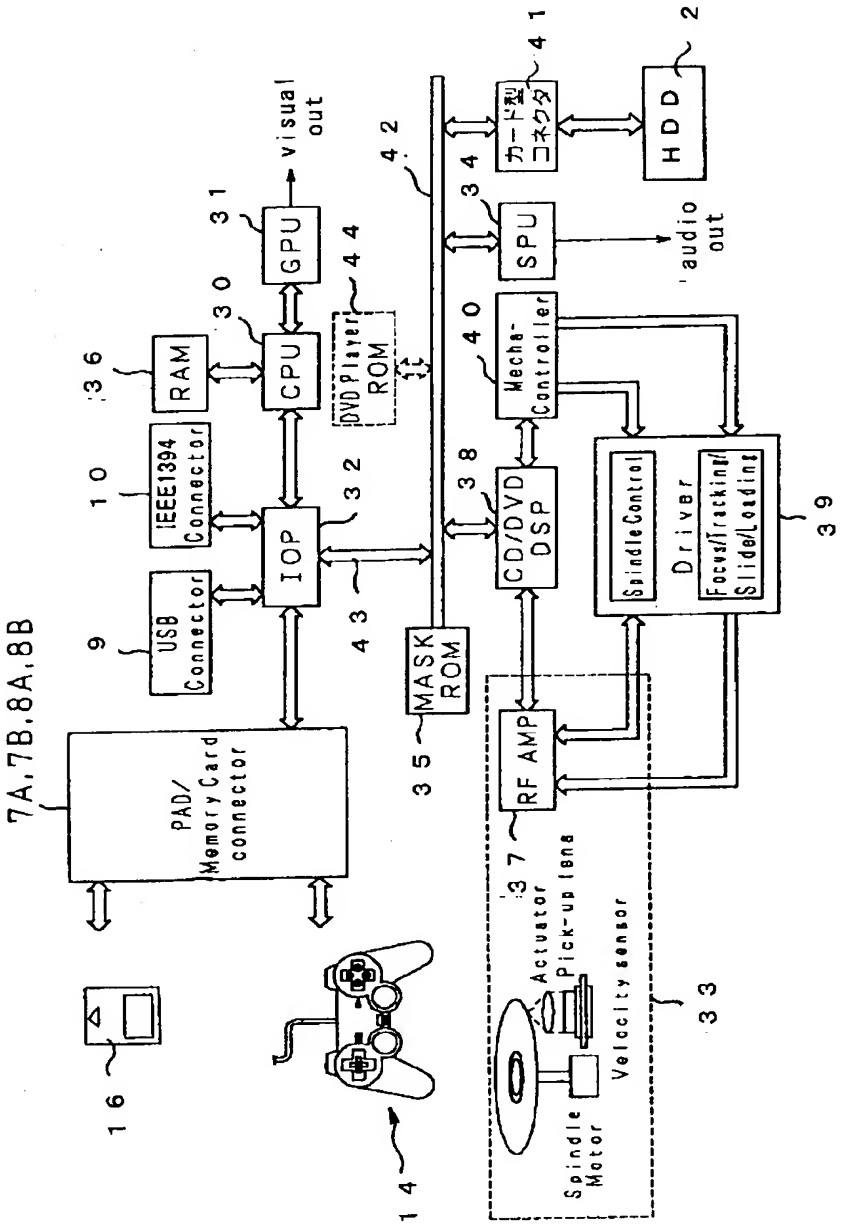
【図４】


Content-Key
Digital Content
Digital Content
Digital Content
対称鍵暗号化
CD／DVD media
media unique ID(MID)
Content-Key
Encrypted Digital Content

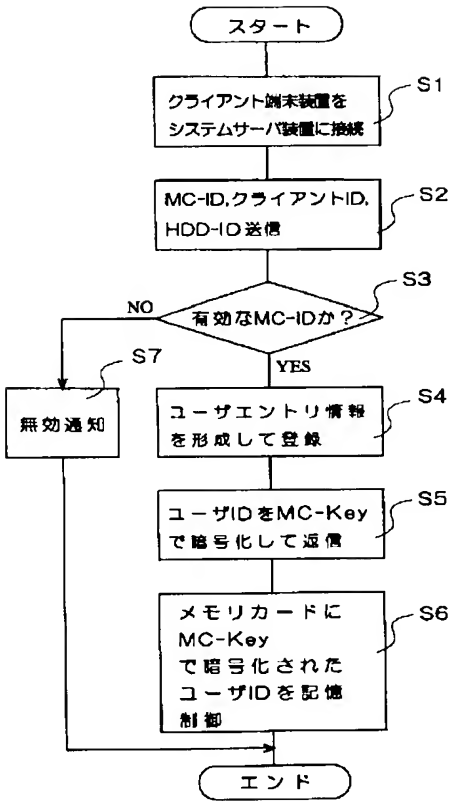
【図８】


media unique ID(MID)
MC－ＩＤ
Content-Key
Encrypted Digital Content
MC-key
UserID
MC-key
mediauniqueID(MID)
システムサーバ装置
1
クライアント端末装置
MC-key
Content-Key
HDD
2
16
MC-key
Content-Key
あらかじめ登録されたMC-keyで暗号化されたContent-Keyリスト
User ID
media unique ID (MID)
MC－ＩＤ
クライアントID
HDD－ID
チェック
インストールflag→ON
既にインストール済みのMIDリスト
ユーザエントリ情報
4
MC-key
Content-Key
Content-Gen-Key
クライアントID
HDD－ID
MC-key
Content-Key
MC-key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD－ID
Memorycard

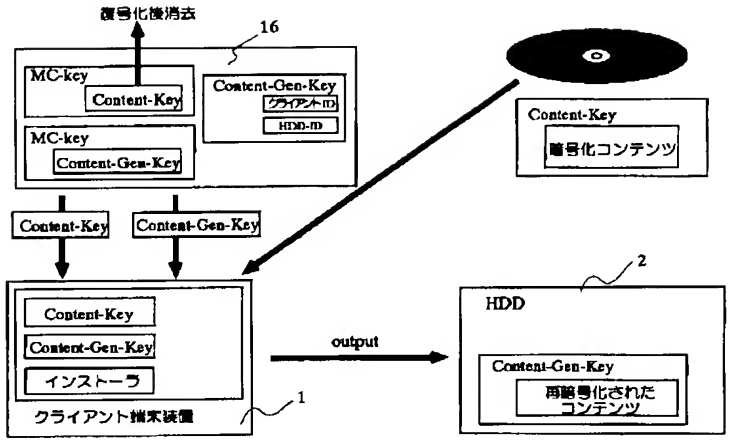
【図３】


7A,7B,8A,8B
PAD/
Memory Card
connector
16
14
USB
Connector
9
IEEE1394
Connector
10
RAM
36
CPU
30
GPU
31
visual
out
IOP
32
43
MASK
ROM
35
42
DVD Player
ROM
44
SPU
34
audio
out
カード型
コネクタ
41
HDD
2
Mecha-
Controller
40
CD/DVD
DSP
38
RF AMP
37
Actuator
Pick-up lens
Velocity sensor
Spindle
Motor
33
Driver
Spindle Control
Focus/Tracking/
Slide/Loading
39

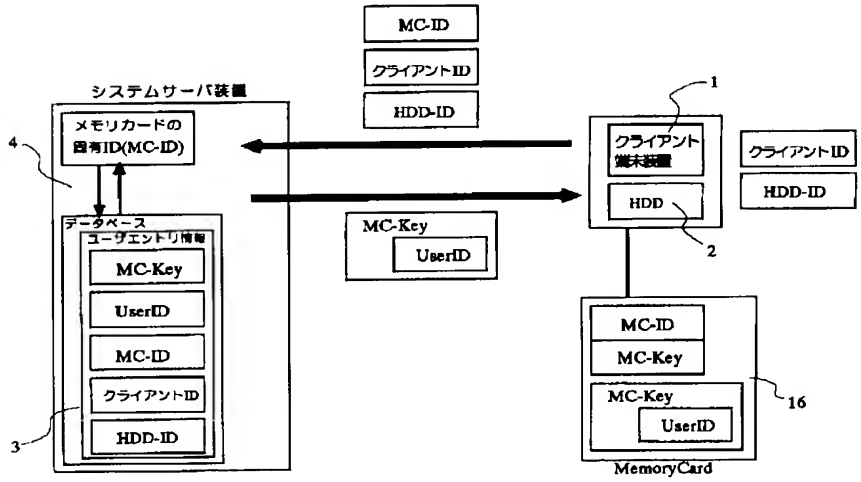
【図５】


スタート
クライアント端末装置をシステムサーバ装置に接続
S1
MC-ID,クライアントID,HDD-ID送信
S2
有効なMC-IDか？
S3
NO
YES
無効通知
S7
ユーザエントリ情報を形成して登録
S4
ユーザIDをMC-Keyで暗号化して返信
S5
メモリカードにMC-Keyで暗号化されたユーザIDを記憶制御
S6
エンド

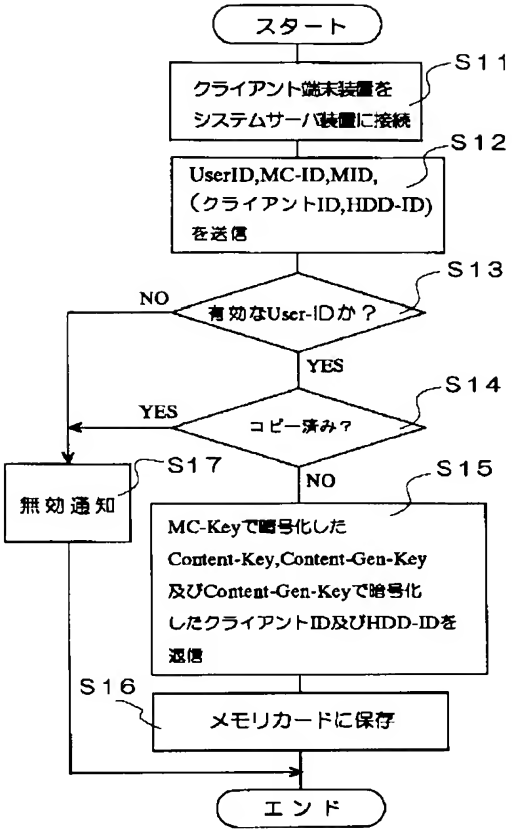
【図１０】


復号化後消去
16
MC-key
Content-Key
MC-key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID
Content-Key
暗号化コンテンツ
Content-Key
Content-Gen-Key
Content-Key
Content-Gen-Key
インストーラ
クライアント端末装置
1
output
2
HDD
Content-Gen-Key
再暗号化されたコンテンツ

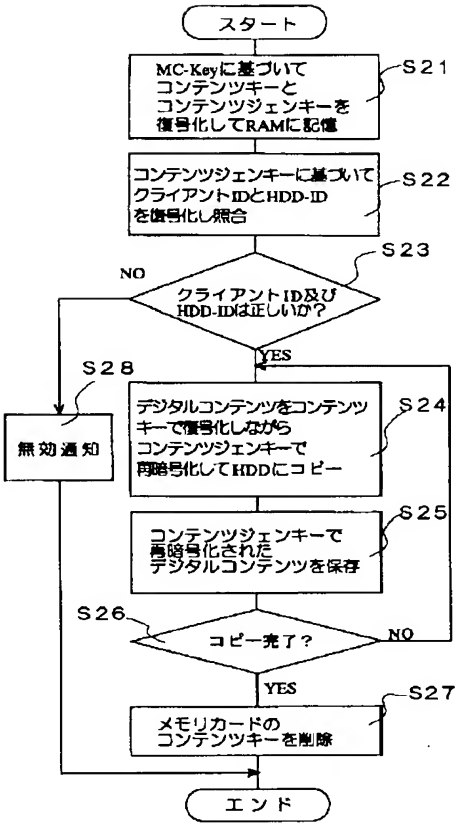
【図６】


MC-ID
クライアントID
HDD-ID
システムサーバ装置
メモリカードの固有ID(MC-ID)
4
データベース
ユーザエントリ情報
MC-Key
UserID
MC-ID
クライアントID
HDD-ID
3
MC-Key
UserID
1
クライアント端末装置
HDD
2
クライアントID
HDD-ID
MC-ID
MC-Key
MC-Key
UserID
16
MemoryCard

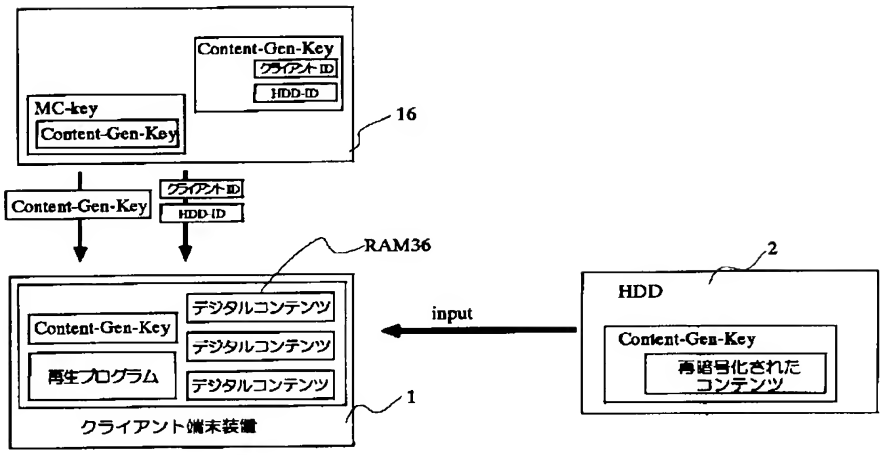
【図７】


スタート
クライアント端末装置を
システムサーバ装置に接続
S11
UserID,MC-ID,MID,
(クライアントID,HDD-ID)
を送信
S12
有効なUser-IDか？
S13
NO
YES
コピー済み？
S14
YES
NO
無効通知
S17
MC-Keyで暗号化した
Content-Key,Content-Gen-Key
及びContent-Gen-Keyで暗号化
したクライアントID及びHDD-IDを
返信
S15
メモリカードに保存
S16
エンド

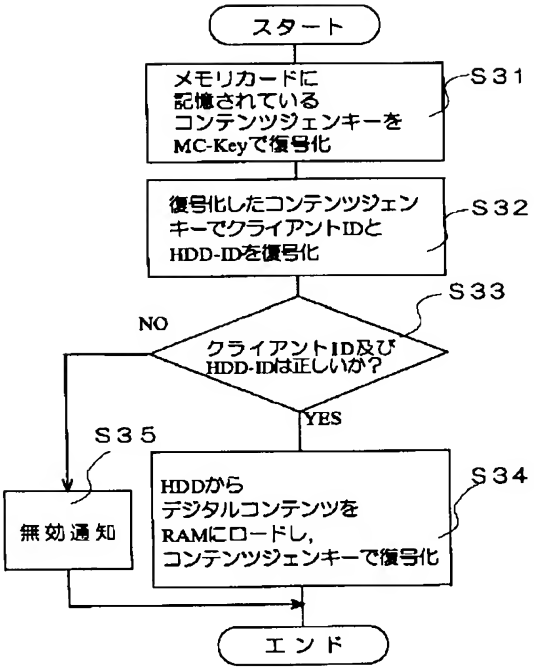
【図９】


スタート
MC-Keyに基づいて
コンテンツキーと
コンテンツジェンキーを
復号化してRAMに記憶
S21
コンテンツジェンキーに基づいて
クライアントIDとHDD-ID
を復号化し照合
S22
クライアントID及び
HDD-IDは正しいか？
S23
NO
YES
無効通知
S28
デジタルコンテンツをコンテンツ
キーで復号化しながら
コンテンツジェンキーで
再暗号化してHDDにコピー
S24
コンテンツジェンキーで
再暗号化された
デジタルコンテンツを保存
S25
コピー完了？
S26
NO
YES
メモリカードの
コンテンツキーを削除
S27
エンド

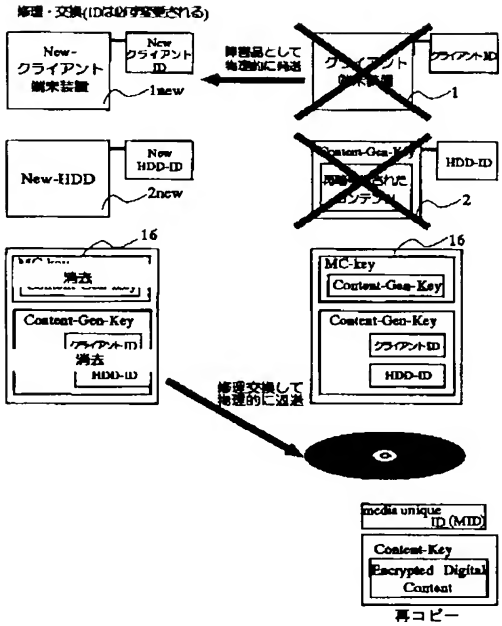
【図１２】


Content-Gen-Key
クライアントID
HDD-ID
MC-key
Content-Gen-Key
16
Content-Gen-Key
クライアントID
HDD-ID
RAM36
Content-Gen-Key
再生プログラム
デジタルコンテンツ
デジタルコンテンツ
デジタルコンテンツ
クライアント端末装置
1
input
2
HDD
Content-Gen-Key
再暗号化された
コンテンツ

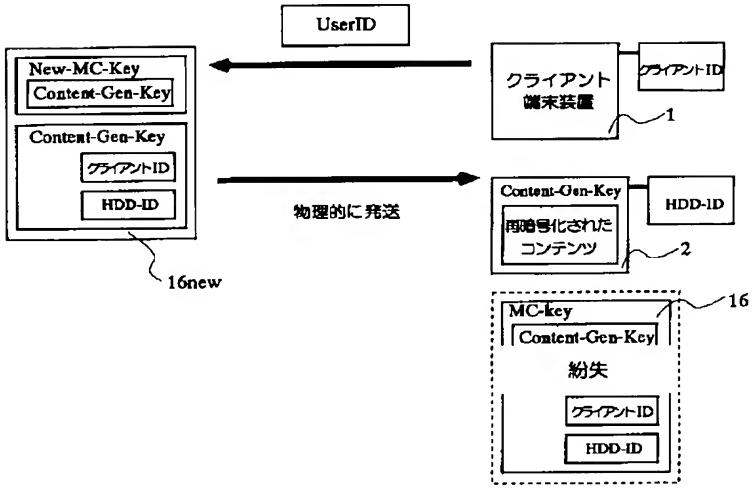
【図１１】


スタート
メモリカードに記憶されているコンテンツジェンキーをMC-Keyで復号化
S31
復号化したコンテンツジェンキーでクライアントIDとHDD-IDを復号化
S32
S33
NO
クライアントID及びHDD-IDは正しいか？
YES
S35
S34
無効通知
HDDからデジタルコンテンツをRAMにロードし，コンテンツジェンキーで復号化
エンド

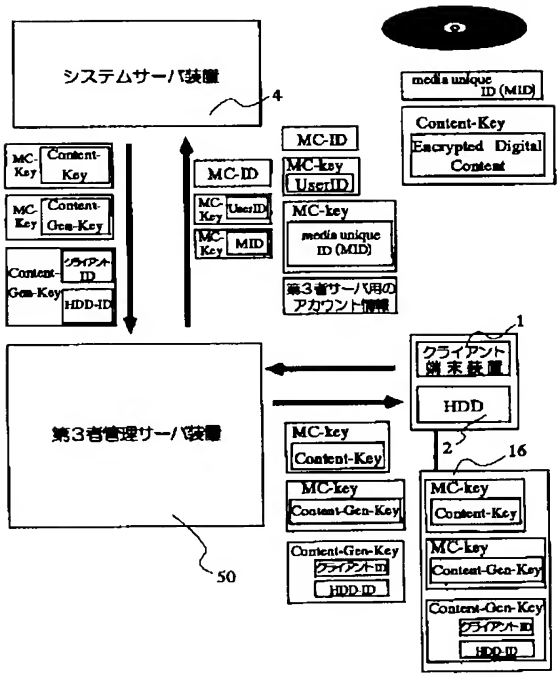
【図１３】


New-クライアント端末装置
New クライアントID
1new
New-HDD
New HDD-ID
2new
クライアントID
HDD-ID
1
2
16
MC-key
Content-Gen-Key
media unique ID (MID)
Content-Key
Encrypted Digital Content
再コピー

【図１４】


UserID
New-MC-Key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID
16new
物理的に発送
クライアント端末装置
クライアントID
1
Content-Gen-Key
再暗号化されたコンテンツ
HDD-ID
2
MC-key
Content-Gen-Key
紛失
クライアントID
HDD-ID
16

【図１５】




【手続補正書】
【提出日】平成１４年８月２０日（２００２．８．２０）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　所定のコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体と、
上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第１の記憶装置にコピーするコピー機能を有し、上記記憶媒体の媒体識別情報と共に、当該端末装置に付された装置識別情報を送信するユーザ端末装置と、
上記媒体識別情報及び上記装置識別情報を受信した際に、該装置識別情報に対応するユーザ端末装置に対して、該媒体識別情報に対応するコンテンツのコピーを許可するコピー許可情報を送信するサーバ装置とを有するコピー管理システム。
【請求項２】　請求項１記載のコピー管理システムであって、
上記サーバ装置は、一つの媒体識別情報に対して１回のみ上記コピー許可情報の送信を行うことを特徴とするコピー管理システム。
【請求項３】　請求項１又は請求項２記載のコピー管理システムであって、
上記ユーザ端末装置は、当該ユーザ端末装置本体に付された端末装置識別情報、上記第１の記憶装置に固有に付された第１の装置識別情報、及びユーザ端末装置を構成する第２の記憶装置に固有に付された第２の装置識別情報のうち、いずれか１つ或いは複数を組み合わせて上記装置識別情報としてサーバ装置に送信することを特徴とするコピー管理システム。
【請求項４】　請求項１から請求項３のうち、いずれか一項記載のコピー管理システムであって、
上記サーバ装置は、上記装置識別情報で暗号化された上記コピー許可情報を送信し、
上記ユーザ端末装置は、上記装置識別情報で、上記暗号化されたコピー許可情報を復号化して用いることを特徴とするコピー管理システム。
【請求項５】　請求項１から請求項４のうち、いずれか一項記載のコピー管理システムであって、
上記ユーザ端末装置は、上記コンテンツのコピー後に、上記コピー許可情報を削除することを特徴とするコピー管理システム。
【請求項６】　請求項１から請求項５のうち、いずれか一項記載のコピー管理システムであって、

上記サーバ装置は、上記コピーするコンテンツを暗号化するための暗号化鍵を送信し、
上記ユーザ端末装置は、上記コンテンツを上記暗号化鍵で暗号化して上記第１の記憶装置にコピーすると共に、上記暗号化鍵を所定の記憶手段に記憶し、該記憶手段に記憶した暗号化鍵を用いて、上記第１の記憶装置にコピーされたコンテンツを復号化して再生することを特徴とするコピー管理システム。
【請求項７】　請求項１から請求項６のうち、いずれか一項記載のコピー管理システムであって、
上記サーバ装置は、上記コピー許可情報の送信が終了した媒体識別情報を、各ユーザのユーザ端末装置に付されている装置識別情報に関連付けてデータベースに記憶し、修理或いは交換によりユーザ端末装置の識別情報が変更された場合、上記データベースに登録されている装置識別情報を、変更された装置識別情報に書き換えることを特徴とするコピー管理システム。
【請求項８】　請求項１から請求項７のうち、いずれか一項記載のコピー管理システムであって、
上記サーバ装置は、上記コピー許可情報の送信を行ったユーザ端末装置を有するユーザに対して所定の課金処理を行うことを特徴とするコピー管理システム。
【請求項９】　請求項１から請求項８のうち、いずれか一項記載のコピー管理システムであって、
上記ユーザ端末装置と上記サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記コピー許可情報をユーザ端末装置に送信した際に、該ユーザに対する課金処理を行う仲介サーバ装置を有することを特徴とするコピー管理システム。
【請求項１０】　記憶されている所定のコンテンツ及び固有の媒体識別情報のうち、該媒体識別情報を読み出すステップと、
ユーザが上記コンテンツのコピーを行う際に使用するユーザ端末装置を構成する装置に対して付された装置識別情報を読み出すステップと、
少なくとも上記読み出した媒体識別情報及び装置識別情報を、所定のサーバ装置に送信するステップと、
上記媒体識別情報及び装置識別情報を送信することで、上記サーバ装置から送信される、上記コンテンツのコピーを許可するコピー許可情報を受信するステップと、
上記受信したコピー許可情報を用いて、上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第１の記憶装置にコピーするステップとを有するユーザ端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項１１】　請求項１０記載の記憶媒体であって、
上記コピー許可情報は、上記送信した装置識別情報で暗号化されており、
上記受信したコピー許可情報を、上記装置識別情報で復号化するステップを有することを特徴とする記憶媒体。
【請求項１２】　請求項１０又は請求項１１記載の記憶媒体であって、
上記コンテンツのコピー後に、上記コピー許可情報を削除するステップを有することを特徴とする記憶媒体。
【請求項１３】　請求項１０から請求項１２のうち、いずれか一項記載の記憶媒体であって、
上記サーバ装置から送信される、上記コピーするコンテンツを暗号化するための暗号化鍵を受信するステップと、
上記コンテンツを、上記暗号化鍵で暗号化してコピーするステップと、
上記暗号化鍵を記憶手段に記憶するステップと、
上記コピーされたコンテンツを再生する際に、上記記憶手段に記憶されている暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップとを有することを特徴とする記憶媒体。
【請求項１４】　請求項１０から請求項１３のうち、いずれか一項記載の記憶媒体であって、
上記媒体識別情報及び装置識別情報を送信するステップでは、ユーザ端末装置本体に付された端末装置識別情報、上記第１の記憶装置に固有に付された第１の装置識別情報、及びユーザ端末装置を構成する第２の記憶装置に固有に付された第２の装置識別情報のうち、いずれか１つ或いは複数を組み合わせて上記装置識別情報として上記サーバ装置に送信することを特徴とする記憶媒体。
【請求項１５】　ユーザ端末装置から送信される、該ユーザ端末装置を構成する装置に付された装置識別情報、及び所定のコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、
対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記受信した媒体識別情報が、上記受信した装置識別情報に関連付けされて登録されているか否かを検出するステップと、
上記受信した媒体識別情報の未登録が検出された際に、上記受信した装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信するステップとを有するサーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項１６】　所定のコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、
ユーザが上記コンテンツのコピーを行う際に使用するユーザ端末装置を構成する装置に対して付された装置識別情報を読み出すステップと、
少なくとも上記読み出した媒体識別情報及び装置識別情報を、所定のサーバ装置に送信するステップと、
上記媒体識別情報及び装置識別情報を送信することで、上記サーバ装置から送信される、上記コンテンツのコピ

ーを許可するコピー許可情報を受信するステップと、
上記受信したコピー許可情報を用いて、上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第１の記憶装置にコピーするステップとを有するユーザ端末装置の情報処理プログラム。

【請求項１７】　ユーザ端末装置から送信される、該ユーザ端末装置を構成する装置に付された装置識別情報、及び所定のコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、
対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記受信した媒体識別情報が、上記受信した装置識別情報に関連付けされて登録されているか否かを検出するステップと、
上記受信した媒体識別情報の未登録が検出された際に、上記受信した装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信するステップとを有するサーバ装置の情報処理プログラム。

【請求項１８】　固有の媒体識別情報が付された記憶媒体に記憶されているコンテンツのコピーを行う際に、該媒体識別情報と共に、ユーザ端末装置を構成する装置に付された装置識別情報を、該ユーザ端末装置からサーバ装置に送信し、
上記サーバ装置において、対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記送信された媒体識別情報が、上記送信された装置識別情報に関連付けされて登録されているか否かを検出し、
上記データベースに、上記媒体識別情報が未登録であった場合に、上記サーバ装置から、上記送信された装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信するコピー管理方法。

---

フロントページの続き

| (51) Int. Cl.[7] | | 識別記号 | FI | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06F | 17/60 | 512<br>ZEC | G06F | 17/60 | 512<br>ZEC |
| H04L | 9/08<br>9/32 | | H04L | 9/00 | 673B<br>601B |

(72)発明者　岡本　伸一
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　吉森　正治
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　犬井　努
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　島川　恵三
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　岡田　豊史
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　九保　亮
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　中村　光宏
東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

Ｆターム(参考)　5B017 AA06 BA05 BA07 CA15
5J104 AA07 AA13 KA02 PA14

(54)【発明の名称】　コピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法